(b) use of your Visa Debit Card to purchase goods or services where a PIN is not required; and

(c) use of your Visa Debit Card or Visa Debit Card Number in a way acceptable to us (for example, to make a transaction over the telephone or internet).

3.3.2. At your request we may attach other services to the Visa Debit Card. Any additional services that you request to be attached to your Visa Debit Card will be advised to you in writing.

3.4. Signing your Visa Debit Card

3.4.1. You agree to sign your Visa Debit Card as soon as you receive it and before using it, as a means of preventing unauthorised use.

3.5. Reporting the loss or theft of your Visa Debit Card

3.5.1. If you believe your Visa Debit Card or PIN record has been lost or stolen, or your PIN has become known to someone else, you should IMMEDIATELY report this by contacting:

(a) DURING NORMAL BUSINESS HOURS (02) 4941 3888. Refer to our website for normal business hours.

(b) OUTSIDE NORMAL BUSINESS HOURS Visa CARD 24hr Emergency Hotline Free Call - 1800 621 199

(c) If you contact the Visa Card 24hr Emergency Hotline:

i. you will be given a reference number which you should retain as evidence of the date and time of your report; and

ii. you should advise us, as soon as you can, that you have made a report to the Visa Card 24hr Emergency Hotline.

3.5.2. If, for any reason any of the above methods of notification is unavailable, any losses occurring due to non-notification will be the liability of Hunter United. To avoid further losses, you are required to continue to try to provide notification of your lost or stolen Visa Debit Card by using one of the methods referred to above. Providing you continue to try and use reasonable endeavours having regard to your own individual circumstances to notify us or the Visa Card 24hr Emergency Hotline, we will continue to be liable for any loss occurring as a result of further unauthorised use of your Visa Debit Card.

3.5.3. If your Visa Debit Card is reported as lost or stolen, we will issue to you a replacement Visa Debit Card. You must give us a reasonable time to arrange cancellation and the issue of a replacement Visa Debit Card.

3.5.4. If the loss, theft or misuse occurs OUTSIDE AUSTRALIA you must notify a financial institution displaying the Visa logo and you must also then confirm the loss, theft or misuse of your Visa Debit Card with us by telephone or priority paid mail as soon as possible.

3.6. Using your Visa Debit Card

3.6.1. Your Visa Debit Card is generally accepted anywhere the Visa logo is displayed in Australia or overseas. We will advise you:

(a) what transactions your Visa Debit Card will enable you to perform at an Electronic Banking Terminal;

(b) which Electronic Banking Terminal networks you may use; and

(c) what mail, internet or telephone transactions you may carry out with your Visa Debit Card by quoting your Visa Debit Card Number.

3.6.2. You may only use your Visa Debit Card to perform transactions on your Linked Account.

3.6.3. If your Visa Debit Card is payWave enabled, then it may be possible for your Visa Debit Card to be used to pay for transactions that are under $100 by using the Visa payWave functionality at Visa payWave participating merchants. Before authorising a Visa payWave transaction by waving your Visa Debit Card over the merchant's enabled Visa payWave terminal, you must check that the correct amount is displayed on the Visa payWave terminal. If your transaction exceeds $100, you will be required to either sign or enter your PIN.

3.6.4. Your Visa Debit Card will be registered with Verified by Visa. Verified by Visa is a program designed to authenticate online transactions. This means when you use your Visa Debit Card online to make a purchase at a Verified by Visa Participating Merchant, your identity may need to be validated if the relevant transaction is deemed to be high risk. In certain circumstances, if your transaction is deemed to be very high risk, the transaction will be declined. If you are unable to validate your identity, your Visa Debit Card may be suspended. For assistance in these circumstances or to learn how your Visa Debit Card may be unsuspended, please contact us during its normal business hours (refer to our website www.hunterunited.com.au for details of our normal business hours).

3.6.5. We do not warrant or accept any responsibility if an Electronic Banking Terminal does not accept

your Visa Debit Card. You should always check with the relevant merchant that it will accept your Visa Debit Card before purchasing any goods or services.

3.6.6. You must not use your Visa Debit Card for any unlawful purpose, including the purchase of goods or services prohibited by the laws of Australia and/or the laws of the location where the Visa Debit Card is used or where the goods or services are provided. Should your Visa Debit Card be used for unlawful purposes, we may restrict you from accessing any available funds from your Linked Account.

3.6.7. It is an offence under Australian law to conduct transactions on an account which may lead to an actual or attempted evasion of a taxation law, or an offence under any other Commonwealth or Territory law. Where we have reasonable grounds to suspect that such transaction(s) have occurred on your Linked Account, we are obliged to report such suspicion to the Australian Transaction Reports and Analysis Centre.

3.6.8. To facilitate the processing of transaction information, your Visa Debit Card details and transaction details may be processed by Visa in countries other than Australia. By using your Visa Debit Card, you agree that information regarding any transactions may be processed outside of Australia.

3.6.9. In the first instance, we will debit your Linked Account (which will reduce the balance of your Linked Account) with the value of all transactions carried out:

(a) by using your Visa Debit Card at an Electronic Banking Terminal;

(b) by using your Visa Debit Card Number (for example, using your Visa Debit Card Number to conduct a telephone or internet transaction); or

(c) when your Visa Debit Card is presented to a merchant (or someone else on behalf of a merchant) in a way acceptable to us.

3.6.10. Fraudulent transactions can arise from use of your Visa Debit Card or Visa Debit Card Number. Where you advise us that a transaction that has been debited (deducted) from your Linked Account is fraudulent, unauthorised or disputed, we will investigate and review that transaction in accordance with section 3.16 of these terms and conditions.

3.6.11. We will also credit your Linked Account (which will increase the balance of your Linked Account) with the value of all deposit transactions processed at Electronic Banking Terminals. We are not responsible in the event that you have a dispute regarding the goods or services purchased using your Visa Card. In the first instance, you should contact the merchant directly. If you cannot resolve the dispute with the merchant, we have the ability in certain circumstances to investigate disputed transactions on your behalf (refer to section 3.16 below for a list of circumstances when we can investigate disputed transactions) and attempt to obtain a refund for you.

3.6.12. If the Linked Account is in the name of more than one person (referred to as a joint account), then you and the joint account holder will be jointly and severally liable (in the first instance) for all transactions carried out by using yours or the joint account holder's Visa Debit Card or Visa Debit Card Number. This means that:

(a) your joint account holder will be liable to us (in the first instance) for all transactions that are carried out by use of your Visa Debit Card or Visa Debit Card Number; and

(b) if applicable, you will be liable to us (in the first instance) for all transactions that are carried out by use of the joint account holder's Visa Debit Card or Visa Debit Card Number.

3.7. Using your Visa Debit Card outside Australia

3.7.1. All transactions conducted overseas will be converted into Australian dollars. Transactions will either be converted directly into Australian dollars or will be first converted from the currency in which the transaction was made into US dollars and then converted to Australian dollars by Visa. The conversion rate used is either:

(a) a rate selected by Visa from a range of rates available in wholesale currency markets for the applicable processing date, which may vary from the rate Visa receives; or

(b) the government-mandated rate in effect for the applicable processing date.

3.7.2. A currency conversion fee may be payable by you when you make a transaction on your Visa Debit Card in a currency other than Australian dollars, or you make a transaction on your Visa Debit Card in any currency (including AUD) that is processed by a card scheme or billed by the merchant outside of Australia. You will be advised by us whether a currency conversion fee applies and the amount of this fee in the *Fees and Charges – Deposit Products and Account Access Facilities* brochure.

3.8. Transaction Limits

3.8.1. You agree that you will NOT use your Visa Debit Card to:

(a) overdraw the balance in your Linked Account; or

(b) exceed the unused portion of any credit limit provided by us under any pre-arranged credit facility.

3.8.2. We:

(a) may set temporary or permanent limits on the minimum and maximum amounts that you may withdraw from your Linked Account on any one day through the Electronic Banking Terminal; and

(b) will advise you of any daily transaction limits that apply at the time of your application of your Visa Debit Card.

3.8.3. Where we impose a temporary minimum or maximum limit, we will use reasonable endeavours to notify you that it has imposed a temporary transaction limit. A temporary maximum transaction limit will usually be imposed in circumstances where transactions appear to be suspicious or fraudulent. Where we impose a new permanent minimum or maximum transaction limit, we will inform you of this change in accordance with the requirements set out in section 2.5 of these terms and conditions.

3.8.4. Merchants offering eftpos facilities have the right to impose conditions on the use of such facilities. This can include imposing their own transaction limits or restrictions on the amount of cash or value that you may obtain using your Visa Debit Card.

3.9. Authorisations and processing of transactions

3.9.1. Certain transactions that you make using your Visa Debit Card may need to be authorised by us before they can proceed. In these circumstances, prior to the transaction being completed, the relevant merchant's financial institution will obtain authorisation from us for the transaction to be processed. Once authorisation is obtained, it will reduce the amount of available funds in your Linked Account. If circumstances occur where authorisation is obtained by us, but the relevant transaction is not completed, your available funds in your Linked Account may be reduced for a period of time.

3.9.2. Transactions will not necessarily be processed to your Linked Account on the same day they occur. The date that you conduct the transaction is referred to as the transaction date. Some transactions will be processed after the transaction date. This is usually due to the relevant merchant's financial institution not processing the relevant transaction on the transaction date.

3.9.3. We have the right to refuse authorisation for you to affect a transaction if:

(a) we have restricted access to your Linked Account in accordance with section 3.12 of these terms and conditions;

(b) in accordance with section 2.9 of these terms and conditions, we believe on reasonable grounds that the transaction is fraudulent or suspicious; or

(c) the transaction will result in you overdrawing your balance in your Linked Account.

3.10. Additional Cards

3.10.1. We may allow you to apply and request that an additional Visa Debit Card be given to your nominee (referred to as an Additional Cardholder). We are not obliged to grant any additional Visa Debit Cards. We are required to comply with all laws governing the issuing of debit cards (including identification and verification of any additional cardholders in accordance with the AML Legislation).

3.10.2. When we issue an additional Visa Debit Card at your request:

(a) you agree that you will provide the Additional Cardholder with a copy of these terms and conditions and any updates we make to these terms and conditions from time to time that are communicated to you;

(b) you will be liable (in the first instance) for all transactions carried out by use of the additional Visa Debit Card. Fraudulent or unauthorised transactions can occur on debit cards. Where you (or your Additional Cardholder) advise us that a transaction that has occurred on your Visa Debit Card or your Additional Cardholder's Visa Debit Card is fraudulent, unauthorised or disputed, we will investigate and review that transaction in accordance with section 3.16 below;

(c) you authorise us to give to any Additional Cardholder information about your accounts for the purposes of their use of the additional Visa Debit Card. You also authorise us to act on the instructions of the Additional Cardholder in relation to their use of their additional Visa

Debit Card, except to the extent that any such instructions relate to the termination of your accounts or the replacement of an additional Visa Debit Card following cancellation of that Visa Debit Card by you; and

(d) you can cancel the additional Visa Debit Card at any time by cutting it in half diagonally and either returning the pieces to us and requesting the additional Visa Debit Card be cancelled or by informing us that you have destroyed the additional Visa Debit Card and disposed of the pieces securely. You must then write to us confirming cancellation of the additional Visa Debit Card. If you cannot destroy the additional Visa Debit Card, you should contact us by telephone and request that we place a "stop" on your Linked Account.

3.10.3. If an Additional Cardholder does not comply with these terms and conditions, then you will be in breach of these terms and conditions (refer to section 3.12 below).

3.11. Renewal of your Visa Debit Card

3.11.1. We will forward to you and your Additional Cardholder a replacement Visa Debit Card before the expiry date of your current Visa Debit Card or additional Visa Debit Card, provided that you are not otherwise in default under these terms and conditions.

3.11.2. If you do not require a replacement Visa Debit Card, either for yourself or an Additional Cardholder, you must notify us before the expiration date of your current Visa Debit Card. You must give us a reasonable time to arrange cancellation of the issue of a replacement Visa Debit Card.

3.11.3. We may issue a new Visa Debit Card to you or your Additional Cardholder at any time. All reissued cards are subject to these terms and conditions. We will typically do this in circumstances where it considers that the security of your Visa Debit Card or PIN may have been compromised or where we are required to issue new cards to all our cardholders as a result of any payment scheme rule changes. In these circumstances, you will not be charged any replacement card fee.

3.12. Cancellation and Return of your Visa Debit Card

3.12.1. The Visa Debit Card always remains the property of Hunter United.

3.12.2. We may cancel your Visa Debit Card and demand the return of the Visa Debit Card issued to you and your Additional Cardholder at any time:

(a) for security reasons where your Visa Debit Card has been or is reasonably suspected by us to have been compromised and such compromise has been caused directly by you, an Additional Cardholder or any other third party as a result of your conduct;

(b) if you breach these terms and conditions or the terms and conditions of the Linked Account and you fail to remedy that default within 14 days after receiving a written notice from us requesting you to remedy the default;

(c) if you close your Linked Account;

(d) if you cease to be a member of Hunter United; or

(e) if you alter the authorities governing the use of your Linked Account (unless we agree).

3.12.3. We may also capture your Visa Debit Card at any Electronic Banking Terminal. In these circumstances, we will notify you that your Visa Debit Card has been cancelled.

3.12.4. We may restrict the ability for you to access any available funds from your Linked Account by using your Visa Debit Card and prevent you and your Additional Cardholders from using your Visa Debit Card in circumstances where:

(a) you are in default in accordance with these terms and conditions; and

(b) we have notified you of this default and advised you that it will restrict access to your Linked Account through use of your Visa Debit Card if you do not rectify the relevant default in accordance with the timeframes set out in the notice, we provided to you.

3.12.5. We, where possible, will provide you with at least seven (7) days' notice of intention to restrict your access to any available funds from your Linked Account by using your Visa Debit Card.

3.13. Conditions after cancellation or expiry of your Visa Debit Card

3.13.1. You must not use your Visa Debit Card or allow your Additional Cardholder to use his or her additional Visa Debit Card:

(a) after it has been cancelled or restricted; or

(b) after the expiry date shown on the face of the Visa Debit Card.

3.13.2. In some circumstances your Visa Debit Card may be used for store purchases which are below certain Floor Limits (which are set by the relevant merchant's financial institution) and where no electronic approvals are in place or if a transaction is processed manually. If you or your Additional Cardholder use your Visa Debit Card after it has been cancelled or restricted in these

circumstances, then you will be liable to us for the value of any transaction as well as any reasonable costs incurred by us in collecting the amounts owing. Any such amounts are immediately due and owing upon demand by us.

3.14. Liability for unauthorised use of or lost or stolen Visa Debit Cards

3.14.1. You are not liable for any loss arising from unauthorised use of your Visa Debit Card:

(a) where the losses are caused by the fraudulent or negligent conduct of:

i. Hunter United;

ii. employees or agents of Hunter United;

iii. companies involved in networking arrangements; or

iv. merchants or agents or employees of merchants;

(b) before you have actually received your Visa Debit Card and/or PIN (including a reissued Visa Debit Card and/or PIN);

(c) subject to section 3.13, where the losses relate to any component of your Visa Debit Card or PIN being forged, faulty, expired or cancelled;

(d) where the losses are caused by the same transaction being incorrectly debited more than once to your Linked Account;

(e) after you have reported your Visa Debit Card lost or stolen or reported the breach of the security of your PIN;

(f) if you did not contribute to any unauthorised use of your Visa Debit Card; or

(g) if the unauthorised transaction was made using your Visa Debit Card information without use of your actual Visa Debit Card or PIN.

3.14.2. For the purpose of section 3.14.1(b), there is a presumption that you did not receive your Visa Debit Card unless we can prove that you received your Visa Debit Card by, for example, obtaining an acknowledgement of receipt from you or (if applicable) obtaining record of you activating your Visa Debit Card.

3.14.3. For the purpose of section 3.14.1(f), we will undertake an assessment to consider whether you have contributed to any loss caused by unauthorised use of your Visa Debit Card. This assessment will include a review of whether you:

(a) voluntarily disclosed your PIN to anyone, including a family member or friend;

(b) voluntarily allowed someone else to observe you entering your PIN into an Electronic Banking Terminal;

(c) wrote or indicated your PIN on your Visa Debit Card;

(d) wrote or indicated your PIN (without making any reasonable attempt to disguise the PIN) on any article carried with your Visa Debit Card or likely to be lost or stolen at the same time as your Visa Debit Card;

(e) allowed anyone else to use your Visa Debit Card;

(f) unreasonably delayed notification of:

i. your Visa Debit Card or PIN record being lost or stolen;

ii. unauthorised use of your Visa Debit Card; or

iii. the fact that someone else knows your PIN; or

(g) in relation to a transaction carried out at an ATM, used an ATM that incorporated reasonable safety standards that mitigated the risk of a card being left in the ATM.

3.14.4. Where a transaction can be made using your Visa Debit Card but does not require your PIN, you are liable only if you unreasonably delay reporting the loss or theft of your Visa Debit Card.

3.14.5. If we can prove on the balance of probability that you have contributed to the unauthorised use of your Visa Debit Card under section 3.14.3 your liability will be the lesser of:

(a) the actual loss when less than your account balance (including the unused portion of any credit limit provided by us under any pre-arranged credit facility);

(b) your account balance (including the unused portion of any credit limit provided by us under any pre-arranged credit facility);

(c) an amount calculated by adding the actual losses incurred for each day or for each relevant period, up to the current daily or other periodic withdrawal limit, on which unauthorised use occurred before you reported the loss, theft or unauthorised use of your Visa Debit Card or breach of PIN security, up to and including the day you make your report; or

(d) the amount for which you would be held liable if any card scheme rules, such as Visa's

scheme rules, applied (if you wish to find out what card scheme rules apply to transactions made using your Visa Debit Card, please contact us).

3.14.6. In assessing your liability under section 3.14.5(c):

(a) where your Visa Debit Card has been lost or stolen, the number of days will be calculated by reference to the day when you should reasonably have become aware that it was lost or stolen; and

(b) the current daily withdrawal limit is the limit applicable at the time of the transaction by reference to the status and/or type of Electronic Banking Terminal at which the transaction occurred.

3.14.7. Where a PIN was required to perform the unauthorised transaction and it is unclear whether or not you have contributed to any loss caused by the unauthorised use of your Visa Debit Card, your liability will be the lesser of:

(a) $150, or a lower figure determined by us;

(b) your account balance (including the unused portion of any credit limit provided by us under any pre-arranged credit facility);

(c) the actual loss at the time we are notified of the loss or theft of your Visa Debit Card or the breach of your PIN security, excluding the portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit; or

(d) the amount for which you would be held liable if any card scheme rules, such as Visa's scheme rules, applied (if you wish to find out what card scheme rules apply to transactions made using your Visa Debit Card, please contact us).

3.14.8. In assessing your liability under this section 3.14:

(a) we will consider all reasonable evidence including all reasonable explanations for an unauthorised use having occurred;

(b) the fact that an account is accessed with the correct PIN, while significant, is not of itself conclusive evidence that you have contributed to the loss;

(c) the use or security of any information required to perform a transaction that you are not required to keep secret (for example, your Visa Debit Card Number and the expiry date on the front of your Visa Debit Card) is not relevant to your liability; and

(d) the portion of losses incurred that you and Hunter United had not agreed could be accessed using the Visa Debit Card and/or PIN that was used to perform the unauthorised transaction shall be excluded from the calculation of your liability.

3.14.9. Your liability for losses occurring as a result of unauthorised use will be determined under the ePayments Code. The guidelines set out at the beginning of these terms and conditions, are the minimum suggested security measures you should take. If you disagree with our resolution process, you should contact us and request that we review our decision in accordance with section 3.16.

3.15. Visa Zero Liability

3.15.1. In addition to the limits placed on your liability pursuant to the ePayments Code and described in section 3.14 above, Visa's scheme rules provide that we shall limit your liability to nil in the following circumstances:

(a) the unauthorised transaction(s) were not affected at an ATM (and will include transaction(s) effected prior to notification of:

i. the unauthorised transaction(s); or

ii. lost or stolen Visa Debit Card, by you to us);

(b) you have not contributed to any loss caused by unauthorised use of your Visa Debit Card as described in section 3.14.3; and

(c) you have provided all reasonably requested documentation to us, which may include provision of a statutory declaration and police report.

3.15.2. Where this Visa Zero Liability section applies, we will endeavour to refund the amount of the unauthorised transaction(s) within five (5) days, subject to:

(a) you having provided all reasonably requested information to us;

(b) you are not otherwise in default or have breached these terms and conditions; or

(c) we have not reasonably determined that further investigation is necessary before refunding the amount of the unauthorised transactions based on:

i. the conduct of the Linked Account;

ii. the nature and circumstances surrounding the unauthorised transaction(s); and

iii. any delay in notifying us of the unauthorised transaction(s).

3.15.3. Any refund is conditional upon the final outcome of our investigation of the matter and may be withdrawn by us where we consider that this section shall not apply as a result of that investigation. In making any determination in respect of this section, we will comply with the requirements of section 3.16 of these terms and conditions.

3.16. Resolving Errors on Account Statements

3.16.1. If you believe a transaction is wrong or unauthorised on your account statement, you must immediately notify us, or the Visa Card 24 Hour Emergency Hot Line as explained in section 3.5. As soon as possible, you must also provide us the following:

(a) your name and address, account number and Visa Debit Card Number;

(b) details of the transaction or the error you consider is wrong or unauthorised;

(c) a copy of the account statement in which the unauthorised transaction or error first appeared;

(d) the dollar amount and an explanation as to why you believe it is an unauthorised transaction or an error;

(e) the names of other users authorised to operate the Linked Account;

(f) details of whether your Visa Debit Card is signed, and PIN is secure; and

(g) any other details required by us.

3.16.2. If we decide that you are liable for all or any part of a loss arising out of unauthorised use of your Visa Debit Card, we will:

(a) give you copies of any documents or other evidence we relied upon; and

(b) advise you whether or not there was any system or equipment malfunction at the time of the transaction.

3.16.3. If we fail to carry out these procedures or cause unreasonable delay, we may be liable for part or all of the amount of the disputed transaction where our failure or delay has prejudiced the outcome of the investigation.

3.16.4. We have the ability to investigate disputed transactions which occur on your Visa Debit Card. The Visa scheme has a dispute resolution process contained in Visa's operating rules. The process sets out specific circumstances and timeframes in which a member of the scheme (for example, us, a bank or another financial institution) can claim a refund in connection with a disputed transaction on a cardholder's behalf. This right is referred to as a "chargeback right". Accordingly, our ability to investigate a disputed transaction on your behalf is limited to the time frames imposed pursuant to the Visa scheme rules. The timeframes vary between 75 days and 120 days, so it is important that you notify us as soon as you become aware of a disputed transaction.

3.16.5. You may wish to dispute a transaction in circumstances where:

(a) the transaction is not recognised by you;

(b) you did not authorise the transaction;

(c) you did not receive the goods or services to which the transaction relates;

(d) the transaction amount differs to the purchase amount;

(e) you did not receive the requested cash from an ATM (or you only received part of the cash requested); or

(f) you believe a transaction has been duplicated.

3.16.6. If you are not happy with the outcome of your query you may make a formal complaint to us. Please see section 2.7 - Complaints and Dispute Resolution for details.

3.17. Malfunction

3.17.1. Other than to correct the error in your Linked Account and the refund of any charges or fees imposed on you as a result, we will not be liable to you for any loss caused by an Electronic Banking Terminal malfunctioning if you were aware, or should have been aware, that the terminal was unavailable for use or was malfunctioning. Where an eftpos Device is not working, the merchant may provide alternative manual processing of the transaction. You will be required to present your Visa Debit Card and sign a voucher. The voucher authorises us to debit your Linked Account with the amount of the transaction (which will reduce the balance in your Linked Account).

3.18. Statements and Receipts

3.18.1. A transaction record slip will be available for each financial transaction carried out with your Visa Debit Card at an Electronic Banking Terminal.
3.18.2. You should obtain, check and retain all transaction record slips including sales and cash advance vouchers issued to you for checking against your account statements.
3.18.3. We will send you an account statement at least every 3 months. You may request more frequent account statements from us.
3.18.4. You may request a copy of your account statement at any time. You should check with us whether fees and charges will apply in these circumstances.

3.19. Assignment

3.19.1. You may not assign your rights under these terms and conditions to any other person. We may assign our rights or transfer the contract to another person where such assignment is to a related party or third party where such third party has a similar or fairer dispute resolution procedure than ours. If we assign or transfer the rights under these terms and conditions, these terms and conditions will apply to the transferee or assignee as if it were named as Hunter United. If we assign these terms and conditions, we will provide you with notice and you will be able to cancel our Visa Debit Card as a result of this assignment without being charged any fees or charges associated with us cancelling your Visa Debit Card.

SECTION 4 – Internet Banking (incl. Mobile Phone Banking & Touchscreen Teller)

Our Internet Banking Facility allows you to perform banking transactions on a variety of devices via the Internet. This section applies if your account permits the attachment of an Internet Banking Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account.

4.1. Internet Banking General Terms

4.1.1. If you do not already have our Internet Banking Facility, you may register for access to this Account Access Facility. Please contact us for more information on how to do this.
4.1.2. The range of services we make available through our Internet Banking Facility will be determined by us in our absolute discretion from time to time. We may extend or reduce this range of services at any time without notice to you.
4.1.3. You must always report any breach of security or misuse of an Account Access Facility by calling us immediately on (02) 4941 3888.
4.1.4. If you unreasonably delay changing your PIN and notifying us of this, your possible loss as a result of unauthorised transactions on your account(s) may increase.
4.1.5. You authorise us to act upon all instructions in relation to the Internet Banking Facility using your Member Number, Access Code, SMS Safecode or External Transfer Code.
4.1.6. We are under no obligation to process any transactions which you make, on the day you make them.
4.1.7. Information about transactions and balances on any account which is available through our Internet Banking Facility may not reflect the current position on that account. We will not be liable for, or in connection with, any inaccuracies in that information.
4.1.8. You agree that any request for a balance or information you make in relation to any account which is regulated by the National Consumer Credit Protection Act is not a request under Section 36 of the Act.
4.1.9. We may from time to time and without notice to you:
(a) place limits on the number or amount of transactions that can be made using our Internet Banking Facility;
(b) change the software, system or equipment required to access the Internet Banking Facility. It is your responsibility to supply and maintain any equipment or software (such as a personal computer, modem or browser) which may be necessary for you to access our Internet Banking Facility.
4.1.10. We may, in our absolute discretion and without notice to you:
(a) refuse to give effect to any instructions received from you in relation to our Internet Banking Facility; or
(b) temporarily suspend access to the Internet Banking Facility.
4.1.11. You must check your account records carefully and promptly. If you believe that there has been a mistake in any transaction using the Internet Banking Facility, or an unauthorised transaction, you must notify us immediately.

4.1.12. You must tell us either in writing or by coming into a branch if you change your residential, postal or email address.
4.1.13. If an account is in more than one person's name, each of you agrees that each person may use the account and have access to account information without any other account holders' consent.
4.1.14. We may terminate your access to the Internet Banking Facility at any time without notice.

4.2. Security

4.2.1. You must keep each of your Member Number, Access Code and External Transfer Code secret. If you do not keep them secret, another person may be able to make transactions on your accounts through the Internet Banking Facility, and we will not be liable for any loss caused as a result of those transactions.
4.2.2. To guard against unauthorised use, it is essential that you:
(a) should not select a numeric code which represents your birth date or an alphabetical code which is a recognisable part of your name;
(b) ensure that no-one knows your Member Number, Access Code or External Transfer Code;
(c) keep any record of your Member Number, Access Code and External Transfer Code in secure places separate from each other and anything which will identify you or your accounts,
(d) ensure that no-one sees or hears your Member Number, Access Code and External Transfer Code when you are using it;
(e) do not leave your computer unattended when you are using the Internet Banking Facility.
4.2.3. You must tell us as soon as possible if you become aware or suspect that:
(a) any of your Member Number, Access Code or External Transfer Codes have been lost, stolen or misused; or
(b) someone may have accessed your accounts without your authority.
(c) You can tell us by Telephoning (02) 4941 3888 or Email enquiries@hunterunited.com.au.
4.2.4. Your Internet Banking Facility has a security level which defines access to your accounts as follows:

Security Level	Access
Level 1	• View Account balances • Transfer within the membership
Level 2 Default Level if mobile number not provided	• View Account balances • Transfer funds within the membership • Transfer funds to any pre- existing external transfer authorities • BPAY to any pre-existing Billers
Level 3*	• View Account balances • Transfer funds within the membership • External transfers • BPAY • Payments to new recipients require the use of an 'External Transfer Code' ** Security access Level 3 no longer available to new Internet Banking registrations.*
Level 4 Default Level if mobile number provided	• View Account balances • Transfer funds within the membership • External transfers • BPAY • Payments to new recipients the use of an 'SMS Safe Code' • PIN change

Level 5	Available to Business Accounts only: • View Account balances • Transfer funds within the membership • External transfers • BPAY • Payments to new recipients require the use of an 'SMS Safe Code' • PIN change

4.2.5. All new members will be given a security access level of 4 unless otherwise indicated in these or other terms and conditions for products or account access facilities.
4.2.6. External fund transfers (including BPAY) to new destinations will require an SMS Safecode in order to affect the transaction. Members on level 3 will require their External Transfer Code. Once the destination has been included in your address book you will not be required to enter the code again.
4.2.7. The SMS Safecode will be sent to the mobile number that you have nominated during registration for SMS Safecode. In order to ensure that you are able to perform external transfers it is your responsibility to ensure that your mobile phone is SMS enabled and available at the time at which you are completing an external transfer.
4.2.8. Your daily limit to initiate transfers outside your membership (excluding BPAY) is set at $5,000 . You may apply to amend (increase or decrease) this limit. Please contact us for more information on how to do this. There are approval conditions on limit requests above $5,000.
4.2.9. You may apply to change your security access level. Please contact us for more information on how to do this.
4.2.10. Memberships opened for non-business customers with a "two to sign" signature authority will be restricted to a security access level of 1.
4.2.11. All external transactions (excluding Osko Payments) are subject to processing cut off times after which payments will not be sent until the next business day
4.2.12. You are solely responsible for providing correct payment details including amount and payee details.
4.2.13. Mistaken Internet Payments will be dealt with in accordance with clause 2.4 above.

4.3. Business Internet Banking

4.3.1. All business internet banking customers will be required to have Level 5.
4.3.2. External fund transfers to new destinations will require an SMS Safecode in order to affect the transaction. Once the destination has been included in your address book you will not be required to enter the code again.
4.3.3. The SMS Safecode will be sent to the mobile number that you have nominated during registration for SMS Safecode. In order to ensure that you are able to perform external transfers it is your responsibility to ensure that your mobile phone is SMS enabled and available at the time at which you are completing an external transfer.
4.3.4. Memberships opened for business customers with a "two to sign" signature authority, who elects to also initiate business internet banking will be responsible for all transactions undertaken by either party on the account. It is your responsibility to ensure the authenticity of all transactions undertaken under this arrangement and Hunter United will not be in anyway liable for unauthorised activities by an authority to the account where there has been a request to access internet banking.
4.3.5. All external transactions (excluding Osko Payments) are subject to processing cut off times after which payments will not be sent until the next business day.

4.4. Liability

4.4.1. Subject to any rights that cannot be excluded by law (including rights under the Trade Practices Act (1974) (Cth)), liability for or in connection with any loss or damage suffered by you or any other person arising directly or indirectly from or in connection with your use of the Internet Banking Facility will be determined by reference to the ePayments Code. This includes but is not limited to loss or damage which may arise as a result of
(a) inaccuracies, errors, omissions or delays in relation to the Internet Banking Facility;
(b) the loss, modification, damage or destruction of hardware or software caused by computer viruses or program bugs or similar causes; or
(c) unauthorised access to your account or any breach of security arising in relation to the Internet Banking Facility;

(d) the failure of our Internet Banking Facility to perform in whole or in part any function which we have specified it will perform;

(e) our Internet Banking Facility being unavailable at any particular time or inaccessible from any particular location;

(f) delays or errors in the execution of any transaction or instruction.

4.4.2. We are not liable for any loss caused as a result of inaccurate information entered by you when using the Internet Banking Facility.

4.4.3. If you do not use the Internet Banking Facility for private or domestic use, our liability is restricted, in accordance with Section 68A of the Trade Practices Act; to:

(a) in the case of goods, the replacement or repair of the goods or the cost of replacing or repairing the goods; or

(b) in the case of services, re-supplying the services or the cost of re- supplying the services.

4.5. Mobile Banking Services

4.5.1. The Internet Banking website has been designed for access via your mobile devices.

4.5.2. You can carry out the following functions via your mobile devices:

(a) View Account balances

(b) View recent transaction history

(c) Transfers funds to other accounts under the logged-on membership

(d) Transfers funds to other existing authorised accounts (internal and external)

(e) BPAY to existing authorised billers < $2,000

SECTION 5 - SMS Alerts

Our SMS Alerts Facility allows you to receive SMS alerts to advise you of activity on your account as it happens. This section applies if your account permits the attachment of a SMS Alerts Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account.

5.1. SMS Alerts Facility General Terms

5.1.1. Hunter United agrees to make the SMS Alerts Facility available to you on the terms and conditions outlined in this document, including those for Internet Banking.

5.1.2. These terms and conditions are in addition to the terms and conditions relevant to your account.

5.1.3. You can register for this facility provided that you

(a) have a Hunter United membership

(b) have a mobile phone capable of SMS and which is for your own exclusive use, and

(c) are authorised to use and incur charges on the mobile device in relation to the facility.

5.1.4. Hunter United may at any time remove, change or impose restrictions on the functionalities of the SMS Alerts Facility in any respect.

5.1.5. There is a limit to the accounts that can be accessed by means of this facility. Only those accounts that can be accessed via Internet Banking can make use of this facility.

5.1.6. You must always report any breach of security or misuse of an Account Access Facility by calling us immediately on (02) 4941 3888.

5.1.7. If you unreasonably delay changing your PIN and notifying us of this, your possible loss as a result of unauthorised transactions on your account(s) may increase.

5.1.8. You acknowledge that SMS Alerts may deliver confidential information to your mobile device. It is your responsibility to protect your device from unauthorised access to the information.

5.1.9. Hunter United excludes all liability for unauthorised access to information contained in the SMS Alerts

5.1.10. You must notify Hunter United immediately if your mobile device used to access and use the facility is lost, stolen, fraudulently accessed or if the mobile number changes.

5.1.11. You should check your account records and statements carefully and promptly notify Hunter United of any apparent discrepancy.

5.1.12. By registering and accessing the SMS Alerts Facility you agree to receive alerts from Hunter United in relation to marketing and promotional offers.

5.1.13. You agree to the use of this facility as an enhanced security mechanism for third party internet banking transactions.

5.1.14. You must ensure that you:

(a) Lock your mobile device or take measures to stop unauthorised use of the facility

(b) Do not provide you mobile device to any other person

(c) Delete the SMS messages you have received from Hunter United once they are no longer required.

5.1.15. You are not liable for any loss caused by the fraudulent or negligent conduct of Hunter United's employees or agents or third parties involved in the provision of the facility or any unauthorised transactions where it is clear that you could not have contributed to the loss.

5.1.16. You are liable for all losses if you have acted fraudulently, either alone or together with any other person.

5.1.17. In respect of joint memberships where there is a requirement for more than one signatory to sign, you agree through registering and accessing the Internet Banking Facility and the SMS Alerts Facility that you understand the implications and liability of allowing one signatory to act on the membership through the use of these facilities. You also indemnify Hunter United for transactions or other action taken by the signatory in using these facilities.

5.2. Access to SMS Alerts Facility

5.2.1. You may register for the facility

(a) through Hunter United's Internet Banking Facility;

(b) by calling (02) 4941 3888; or

(c) in any other methods made available by Hunter United from time to time.

5.2.2. A request to register for the facility will be approved by Hunter United at its discretion.

5.2.3. Access to the facility may be denied, cancelled or suspended for any reason without immediate notice to you.

5.2.4. Hunter United can suspend or cancel access to the facility described in these terms and conditions without giving you notice and without being responsible for any loss which you suffer as a result.

5.2.5. Hunter United may cancel or suspend the facility in instances such as but not limited to:

(a) unpaid SMS Alerts charges

(b) suspected fraudulent activity in relation to the facility or the membership generally

(c) repeated failure to send SMS Alerts to nominated mobile number

SECTION 6 – BPAY

Our BPAY Facility is available over the counter in our branches or via Internet Banking (including Mobile Phone Banking and Touchscreen Teller) and allows you to pay bills which carries the BPAY logo. This section applies if your account permits the attachment of a BPAY Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account.

6.1. BPAY General Terms

6.1.1. You must always report any breach of security or misuse of an Account Access Facility by calling us immediately on (02) 4941 3888.

6.1.2. If you unreasonably delay changing your PIN and notifying us of this, your possible loss as a result of unauthorised transactions on your account(s) may increase.

6.1.3. Although we take all precautions with respect to BPAY transactions, the security of electronic funds transfer transactions can never be guaranteed. Particularly in electronic mediums such as the internet, there is always a risk of interception of data by a rogue or hacker.

6.1.4. We receive a commission on BPAY transactions, please see our *Financial Services Guide* on our website for details.

6.2. Payments

6.2.1. We will not accept an order to stop a BPAY Payment once you have instructed us to make that BPAY payment.

6.2.2. You should notify us immediately if you become aware that you may have made a mistake (except for a mistake as to the amount you mean to pay - for those errors see section 6.2.6) when instructing us to make a BPAY Payment, or if you did not authorise a BPAY Payment that has been made from your account. Section 6.3 describes when and how we will arrange for such a BPAY Payment (other than in relation to a mistake as to the amount you must pay) to be refunded to you.

6.2.3. Subject to section 6.10 - "Cut-off Times", Billers who participate in the BPAY scheme have agreed that a BPAY Payment you make will be treated as received by the Biller to whom it is

directed:

(a) on the date you make that BPAY Payment before our Payment Cut-Off time on a Banking Business Day; or

(b) on the next Banking Business Day if you tell us to make a BPAY Payment after our Payment Cut-Off time on a Banking Business Day, or on a non-Banking Business Day.

6.2.4. A delay might occur in the processing of a BPAY Payment where:

(a) there is a public or bank holiday on the day after you tell us to make a BPAY Payment;

(b) you tell us to make a BPAY Payment either on a day which is not a Banking Business Day or after the Payment Cut-off Time on a Banking Business Day;

(c) another financial institution participating in the BPAY Scheme does not comply with its obligations under the BPAY Scheme; or

(d) a Biller fails to comply with its obligations under the BPAY Scheme.

6.2.5. While it is expected that any delay in processing under this agreement for any reason set out in section 6.2.4 will not continue for more than one Banking Business Day, any such delay may continue for a longer period.

6.2.6. You must be careful to ensure that you tell us the correct amount you wish to pay. If you instruct us to make a BPAY Payment and you later discover that:

(a) the amount you told us to pay was greater than the amount you needed to pay, you must contact the Biller to obtain a refund of the excess; or

(b) the amount you told us to pay was less than the amount you needed to pay, you can make another BPAY Payment for the difference between the amount actually paid to a Biller and the amount you needed to pay.

6.3. Liability for mistaken payments, unauthorised transactions and fraud

6.3.1. We will attempt to make sure that your BPAY Payments are processed promptly by the participants in the BPAY Scheme, including those Billers to whom your BPAY Payments are to be made. You must tell us promptly if:

(a) you become aware of any delays or mistakes in processing your BPAY Payments

(b) you did not authorise a BPAY Payment that has been made from your account, or

(c) you think that you have been fraudulently induced to make a BPAY Payment

We will attempt to rectify any such matters in relation to your BPAY Payments in the way described in this section. However, except as set out in this section 6.3 and section 6.13, we will not be liable for any loss or damage you suffer as a result of using the BPAY Scheme. Liability for loss or damage will be determined by reference to the ePayments Code.

6.3.2. If a BPAY Payment is made to a person or for an amount which is not in accordance with your instructions (if any), and your account was debited for the amount of that payment, we will credit that amount to your account. However, if you were responsible for a mistake resulting in that payment and we cannot recover within 20 Banking Business Days of us attempting to do so the amount of that payment from the person who received it, you must pay us that amount.

6.3.3. If a BPAY Payment is made in accordance with a payment direction which appeared to us to be from you or on your behalf but for which you did not give authority, we will credit your account with the amount of the unauthorised payment. You must pay the amount of that unauthorised payment if:

(a) we cannot recover within 20 Banking Business Days of us attempting to do so that amount from the person who received it, and

(b) the payment was made as a result of a payment direction which did not comply with our prescribed security procedures for such payment directions.

6.3.4. If a BPAY Payment is induced by the fraud of a person involved in the BPAY Scheme, then that person should refund you the amount of the fraud- induced payment. However, if that person does not refund you the amount of the fraud induced payment, you must bear the loss unless some other person involved in the BPAY Scheme knew of the fraud or would have detected it with reasonable diligence, in which case that person must refund you the amount of the fraud-induced payment.

6.3.5. If a BPAY Payment you have made falls within the type described in section 6.3.3 and also Section 6.3.2 or 6.3.4, then we will apply the principles stated in section 6.3.3. If a BPAY Payment you have made falls within both the types described in section 6.3.2 and 6.3.4, then we will apply the principles stated in section 6.3.4.

6.3.6. You indemnify us against any loss or damage we may suffer due to any claim, demand or action of any kind brought against us arising directly or indirectly because you:

(a) did not observe any of your obligations under these terms and conditions; or

(b) acted negligently or fraudulently in connection with this agreement.

6.3.7. If you tell us that a BPAY Payment made from your account is unauthorised, you must first give us your written consent addressed to the Biller who received that BPAY Payment, consenting to us obtaining from the Biller information about your account with that Biller or the BPAY Payment, including your customer reference number and such information as we reasonably require to investigate the BPAY Payment. We are not obliged to investigate or rectify any BPAY Payment if you do not give us this consent.

6.4. BPAY Scheme

6.4.1. Hunter United is an Associate member of the BPAY Scheme. The BPAY Scheme is an electronic payments scheme through which you can ask us to make payments on your behalf to organisations ("Billers") who tell you that you can make payments to them through the BPAY Scheme ("BPAY Payments"). We will tell you if we are no longer a Member of the BPAY Scheme.

6.4.2. When you tell us to make a BPAY Payment, you must give us the information specified in section 6.7 below. We will then debit (your account/ the account you specify) with the amount of that BPAY Payment.

6.5. How to use the BPAY Scheme

6.5.1. You can make a BPAY Payment by: -

(a) Internet Banking (including Mobile Phone Banking for authorised Billers <$2,000 and Touchscreen Teller); or

(b) Branch counter transaction.

6.5.2. The payer acknowledges that the receipt by a Biller of a mistaken or erroneous payment does not or will not constitute under any circumstances, part or whole, satisfaction of any underlying debt owed between the payer and that Biller.

6.5.3. You must register with us if you wish to use Hunter United's Internet Banking. See section 4.1.1 above.

6.6. Valid payment direction

6.6.1. We will treat your instruction to make a BPAY Payment as valid if, when you give it to us, you comply with these *Account Access Terms and Conditions* and the terms and conditions for your account.

6.7. Information you must give us

6.7.1. The information you must give us to instruct us to make a BPAY Payment is:

(a) valid Biller Code;

(b) valid Reference Number;

(c) the amount to be paid; and

(d) details of the account to be debited.

You acknowledge that we shall not be obliged to affect a BPAY Payment if you do not give us all of the above information or if any of the information you give us is inaccurate.

6.8. Payment queries

6.8.1. Payment queries can be directed to any branch of Hunter United. Disputed transactions will be dealt with in terms of section 2.7.

6.9. Suspension

6.9.1. We may suspend your right to participate in the BPAY Scheme at any time.

6.9.2. Suspension may apply:

(a) if you do not make a payment in accordance with the terms and conditions for BPAY or the Internet Banking Facility; or

(b) If the payer or someone acting on their behalf is suspected of being fraudulent.

6.10. Cut-off times

6.10.1. If you tell us to make a payment before the time specified below, it will in most cases be treated as having been made on the same day.

6.10.2. Cut-off time: 4.00pm

6.10.3. However, the payment may take longer to be credited to a Biller if you tell us to make a payment on a Saturday, Sunday or a public holiday or if another participant in the BPAY Scheme does not process a payment as soon as they receive details.

6.11. When a Biller cannot process a payment

6.11.1. If we are advised that your payment cannot be processed by a Biller, we will:

(a) advise you of this;

(b) credit your account with the amount of the BPAY Payment; and

(c) take all reasonable steps to assist you in making the BPAY Payment as quickly as possible.

6.12. Account records

6.12.1. You should check your account records carefully and promptly report to us, as soon as you become aware of them, any BPAY Payments that you think are errors or are BPAY Payments that you did not authorise or you think were made by someone else without your permission.

6.13. Consequential damage

6.13.1. We are not liable for any consequential loss or damage you suffer as a result of using the BPAY Scheme, other than due to any loss or damage you suffer due to our negligence or in relation to any breach of a condition or warranty implied by law in contracts for the supply of goods and services and which may not be excluded, restricted or modified at all or only to a limited extent.

6.14. BPAY View

Our BPAY View Facility is available via Internet Banking (including Mobile Phone Banking and Touchscreen Teller) and allows you to receive, view and pay your bills which carry the BPAY logo. This section applies if your account permits the attachment of an Internet Banking Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account.

6.14.1. You register for BPAY View by simply registering Biller information via Internet Banking.

6.14.2. If you register with BPAY View, you:

(a) agree to our disclosing to Billers nominated by you:

i. such of your personal information (for example your name, email address and the fact that you are our customer) as is necessary to enable Billers to verify that you can receive bills and statements electronically using BPAY View (or telling them if you cease to do so); and

ii. that an event in section 6.14.3(b), 6.14.3(c), 6.14.3(d), 6.14.3(e), or 6.14.3(f) has occurred;

(b) agree to us or a Biller (as appropriate) collecting data about whether you access your emails, our Website and any link to a bill or statement;

(c) agree to receive bills and statements electronically and agree that this satisfies the legal obligations (if any) of a Biller to give you bills and statements. For the purposes of this section we are the agent for each Biller nominated by you under 6.14.2(a) above.

6.14.3. You may receive paper bills and statements from a Biller instead of electronic bills and statements:

(a) at your request to a Biller (a fee may be charged by the applicable Biller for supplying the paper bill or statement to you if you ask for this in addition to an electronic form);

(b) if you or a Biller de-register from BPAY View;

(c) if we receive notification that your email mailbox is full, so that you cannot receive any email notification of a bill or statement;

(d) if your email address is incorrect or cannot be found and your email is returned to us undelivered;

(e) if we are aware that you are unable to access your email or our website or a link to a bill or statement for any reason; and

(f) if any function necessary to facilitate BPAY View malfunctions or is not available for any reason for longer than 3 business working days.

6.14.4. You agree that when using BPAY View:

(a) if you receive an email notifying you that you have a bill or statement, then that bill or statement is received by you:

7.1.7. It is your responsibility to make good any HU EzyPay payments that have not been made for any reason.
7.1.8. You can stop a HU EzyPay payment by giving us notice up to and including the due date you have specified for the payment providing the payment has not been made. This can be done via Internet Banking or by contacting a Hunter United Branch.
7.1.9. To make sure your HU EzyPay payment reaches its destination on time, make sure the due date for the HU EzyPay payment is at least 5 days before the payment falls due.
7.1.10. Initiating external transfers to other institutions or initiating transfer of funds between Hunter United memberships using the Internet Banking facilities are limited to a total of $5,000 per membership per day. If you wish to vary your daily transfer limit below or above $5,000, you will need to complete an application to do so. Please contact us for more information on how to do this. There are approval conditions on limit requests above $5,000.
4.2.14. We cannot be held responsible for delays in making payments and any loss you suffer due to postal or electronic communication systems.
4.2.15. You are solely responsible for providing correct payment details including amount and payee details.
4.2.16. Mistaken Internet Payments will be dealt with in accordance with clause 2.4 above.

SECTION 8 – Cheques

This section applies if your account permits the drawing of a Hunter United Corporate Cheque or KDVD Cheque Book Facility DWWDFKHG. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if these Payment Facilities are available on your account.

8.1 Hunter United Corporate Cheque

8.1.1. A Hunter United Corporate Cheque is issued by the Commonwealth Bank of Australia and drawn on our account.
8.1.2. A fee is charged for each Hunter United Corporate Cheque issued.
8.1.3. You can only obtain a Hunter United Corporate Cheque from one of our branches. A Cheque Withdrawal form must be completed and signed.
8.1.4. The Available Balance (as defined in section 8.1.5 below) of your account at the time the cheque is drawn, must be sufficient to cover the cheque value and fee.
8.1.5. The “Available Balance” includes any funds in your account, any unused overdraft or other agreed credit facility made available for your account. The Available Balance does not include deposits received but uncleared in accordance with the policy of Hunter United, nor does it include interest accrued but not credited or deposits in transit.
8.1.6. If the signature of an officer of Hunter United is forged or placed on a Hunter United Corporate Cheque without our authority, we are not legally liable for the cheque concerned.
8.1.7. Hunter United will dishonour a Hunter United Corporate Cheque that has been fraudulently and/or materially altered.
8.1.8. If your Hunter United Corporate Cheque is lost or stolen, please immediately notify us by calling (02) 4941 3888 or visiting a Hunter United Branch.
8.1.9. You can request to stop payment on a Hunter United Corporate Cheque. See section 8.7 below.

8.2 Cheque Book Facility

8.2.1. These Cheque Book Facility terms and conditions relate to existing Cheque Book Facilities. Hunter United accounts. These terms
8.2.2. In signing the Cheque Account Application Form or upon prior issue by you of a cheque or the making of a deposit under the Cheque Book Facility you acknowledge that (subject to acceptance by us) you agree to these terms and conditions and that you have appointed both Hunter United and Indue Ltd ("Indue") as your agent and that you have authorised each of them to: -

(a) Conduct accounts ("the Bank Account") with Westpac Banking Corporation ("the Bank") to enable you to draw cheques for payment for goods and services out of the funds in your account with Hunter United which is dedicated either exclusively or otherwise to the Cheque Book Facility (the "Hunter United Account") and make deposits to the Bank in accordance with these terms and conditions; and

(b) Transfer funds to the Bank Account from your Hunter United Account to meet the amount of cheques or payment orders ("a cheque") that you or your Authorised Signatories have signed and meet the value of all costs, taxes or charges made or incurred by us or the Bank.

(c) Disclose to the Bank such information relating to your Hunter United Account as is necessary to process all transactions carried out by you.

8.3 Cheque Book Facility General Terms

8.3.1. You acknowledge that the Bank may refuse to pay or dishonour any cheque that is drawn by you under the Cheque Book Facility and presented for payment, regardless of the state of your account with your Hunter United Account if:

(a) the Bank receives a direction from Indue to dishonour the cheque, whether or not such direction is authorised or justified;

(b) at the time of presentment of the cheque, or at any time within which the cheque may be dishonoured under the then current practice of bankers:

i. Indue fails or omits to pay to the Bank, an amount in cleared funds equal to the face value of the cheque;

ii. A petition is lodged or an order is made or a resolution is passed for the winding up of Indue or placing it under official management or any ground for its winding up has arisen or any meeting is convened for the purpose of considering any such resolution or any resolution for any arrangement or composition with creditors or a receiver of its undertaking or property or any part thereof is appointed or an Administrator is appointed or it stops payment generally or without the consent of the Bank ceases or threatens to cease to carry on business or a major part thereof;

(c) the cheque drawing and deposit facility is terminated.

8.3.2. The Bank may disclose to us and to Indue all information relating to your participation in the Cheque Book Facility and the transactions effected on your behalf.

8.3.3. You will pay charges as shall be determined by us from time to time in relation to all transactions and to all cheques drawn on or deposits made to the Bank pursuant to the Cheque Book Facility.

8.3.4. You agree that the rights and liabilities of Hunter United in relation to its services pursuant to the Cheque Book Facility shall be as if Hunter United were a drawee institution as defined in the Cheques Act 1986.

8.3.5. You must always report any breach of security or misuse of an Account Access Facility by calling us immediately on (02) 4941 3888.

8.3.6. Any cheque received by us before we receive a written notice of cancellation or variation of authority may be paid by us in the normal course of business.

8.3.7. We reserve the right to withdraw the cheque drawing and deposit facility at any time. No cheques may be issued by you after the facility has been withdrawn.

8.3.8. If your Hunter United Account is held in the name of two (2) or more persons, all funds in that account will be held jointly. The expression "member" includes all such persons jointly and severally. If one of the parties should die, any balance in these accounts shall accrue in accordance with the law of survivorship for the time being in the State in which Hunter United is incorporated.

8.3.9. In the event that a correctly authorised and presented cheque exceeds the available balance of your Hunter United Account, you hereby authorise us, (but we are under no obligation so to do), to transfer to that account from any other account or accounts held with us in your name(s), sufficient funds (within the Available Balance, as defined in section 8.3.10, of such other account or accounts) to allow payment of the cheque. We may, at our absolute discretion, debit a fee, as determined by us from time to time, to your Hunter United Account for each and every such transfer, and such fee shall be a debt from you to us. Notwithstanding this condition, we shall be held harmless from any claim whatsoever from you or any other person or organisation, should we fail or refuse to make such a transfer.

8.3.10. The “Available Balance” for the purposes of the Cheque Book Facility, includes any funds lodged in your Hunter United Account, any unused overdraft or other agreed credit facility made available for your Hunter United Account. The Available Balance does not include deposits received but uncleared in accordance with the policy of Hunter United, nor does it include interest accrued but not credited or deposits in transit.

8.3.11. If we, for any reason and without reference to you, pay a correctly authorised and presented cheque that exceeds your Available Balance, then you shall incur a debt to us for the amount by which the cheque exceeds the Available Balance. In such circumstances, the debt shall be repayable by you immediately upon the written demand of Hunter United. If you fail to repay such debt, then you shall be required to pay all costs and expenses whatsoever incurred by us in collection of that debt.

8.3.12. There is no cheque encashment facility available. That is, cheques cannot be cashed at Hunter United offices and must be deposited to an account.

8.3.13. You may make deposits to your Hunter United Account at any branch of the Westpac Bank using the deposit forms included at the back of your cheque book. Deposits lodged with the Westpac Bank may not be drawn against until they have been credited to your Hunter United Account. This should take no more than five (5) days.

8.3.14. If your cheque book is lost or stolen, please immediately notify us by calling (02) 4941 3888 or

visiting any Hunter United Branch.

8.4 Writing personal cheques

8.4.1. It is your responsibility to ensure that all cheques drawn by you are properly authorised and completed. Any cheque presented for payment which is undated; unsigned or without a payee included may be dishonoured.

8.4.2. When filling in a cheque, to reduce the risk of forgery or unauthorised use, you should always:

(a) start the name of the person to whom you are paying the cheque as close as possible to the word 'Pay';

(b) draw a line from the end of the person's name to the beginning of the printed words 'or bearer';

(c) start the amount in words with a capital letter as close as possible to the words 'The sum of' and do not leave blank spaces large enough for any other words to be inserted; also add the word 'only' after the amount in words;

(d) draw a line from the end of the amount in words to the printed '$';

(e) start the amount in numbers close after the printed '$' and avoid any spaces between the numbers;

(f) always add a stop '.' or dash '-' to show where the dollar's end and the cents begin and, if there are no cents, always write '.00' or '-0' to prevent insertion of more numbers to the dollar figure.

8.5 Crossing a personal cheque 'not negotiable' or 'account payee only'

8.5.1. If you cross a cheque, it is a direction to your financial institution to pay the cheque into an account at a bank or other financial institution. A crossing does not actually prevent the cheque being negotiated or transferred to a third party before presentation to a bank or financial institution for payment.

8.5.2. 'Not Negotiable' crossing. Crossing a cheque means drawing 2 lines clearly across the face of the cheque. When you cross a cheque or add the words 'not negotiable' between the crossing, you may be able to protect yourself, but not always, against theft or fraud. This crossing sometimes serves as a warning to the collecting financial institution, if there are other special circumstances that it should inquire if its customer has good title to the cheque.

8.5.3. 'Account Payee' crossing. When you add the words' account payee only' between these lines you are saying that only the named person can collect the proceeds of the cheque. These words may give you better protection against theft or fraud. It would be prudent for the collecting financial institution to make inquiries of the customer paying the cheque in, if the customer is not the payee of the cheque.

8.6 Deleting 'or bearer' on a personal cheque

8.6.1. Your pre-printed cheque forms have the words 'or bearer' after the space where you write the name of the person to whom you are paying the cheque. The cheque is a 'bearer' cheque.

8.6.2. If you cross out the words 'or bearer' and do not add the words 'or order', the cheque is still a bearer cheque. You can give yourself more protection against theft or fraud by crossing out the words 'or bearer' and adding the words 'or order'.

8.7 Stopping a Hunter United Corporate Cheque or personal cheque

8.7.1. If you want to stop payment on any cheque, you must provide sufficient particulars to identify the cheque and advise us before the cheque is presented for payment.

8.7.2. We are only required to instruct a stop payment on any cheque when our standard stop payment notice has been correctly completed, signed and delivered to us. Stop Payment Forms are available from our branches, by calling (02) 4941 3888 or emailing enquiry@hunterunited.com.au.

8.7.3. You must indemnify us against all claims or any loss and cost we may incur as a result of the stopped payment.

8.7.4. You must notify us in writing if you wish to cancel the stop payment request.

8.7.5. A fee is charged for each stop payment on personal cheques and Hunter United Corporate Cheques.

8.8 Dishonouring a personal cheque

8.8.1. It is your responsibility to ensure there are sufficient funds in your account to cover the cheque(s)

presented for payment.

8.8.2. If the amount of any cheque presented for payment to the Bank exceeds the Available Balance (as defined in section 8.3.10) in your Hunter United Account at the time the cheque is presented, we may instruct the Bank to refuse to pay the cheque. In such event, we will advise you in writing, by ordinary pre-paid post, as soon as practicable, but will incur no liability for failure to do so.

8.8.3. Where the Bank refuses to pay a cheque in accordance with this condition, or in accordance with any other condition, we may, at our absolute discretion, debit to your Hunter United Account any costs incurred through such refusal, any such costs shall be a debt from you to us.

8.8.4. A fee is charged for each personal cheque or deposited cheque that is dishonoured.

8.8.5. We may also dishonour your cheque or not pay on it if:

(a) you have not drawn up the cheque clearly, so we are unsure of what you want it to do;

(b) you have post-dated your cheque and it is presented for payment before the date on the cheque; or

(c) the cheque is 'stale', that is, the date of the cheque is more than 15 months ago; or we have notice of your death or mental incapacity.

SECTION 9 – PayID

Our PayID Facility is available via Internet Banking (including Mobile Phone Banking and Touchscreen Teller) and allows you to receive NPP Payments using an identifier (e.g. mobile number or email address). This section applies if your account permits the use of the PayID Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account.

9.1 PayID General Terms

9.1.1. PayID is the NPP Payment addressing service that enables NPP Payments using an alternative identifier (e.g. mobile number or email address) instead of a BSB and account number.

9.1.2. You do not need to create a PayID to make or receive Osko Payments. BSB and account numbers can be used instead.

9.1.3. Not all financial institutions, accounts and payment types support payments to a PayID.

9.2 Registering (creating) your PayID

9.2.1. Consult your account's Product Key Fact Sheet to determine if you can link a PayID to your account.

9.2.2. You can register a PayID through our Internet Banking Facility. We will not register a PayID for you without your prior consent.

9.2.3. You may register a PayID provided it is a supported PayID type. We currently support mobile phone numbers or email addresses. We may update this list from time to time.

9.2.4. Before registering your PayID you must confirm that:

(a) you have the right to use your PayID;

(b) your PayID is and account details are accurate and up-to-date; and

(c) you agree to your PayID details being stored with the PayID Service.

9.2.5. You must satisfy us that you own or are authorised to use your chosen PayID before you can use it to receive NPP Payments. This means we may ask you to provide evidence to establish this to our satisfaction, whether you are already registered for any other mobile or online banking or online payment services with us or not.

9.2.6. When you register your PayID, your account name will be registered as your PayID Name. Depending on the policy of a payer's financial institution, your PayID Name may be displayed to payers who send you a NPP Payment.

9.2.7. Once a PayID is registered and linked to your account, it may not be used in relation to any other account with us or with any other financial institution. See below for details on transferring your PayID.

9.2.8. You can choose to link more than one PayID to your account. E.g. both your mobile and email address can be linked to the same account. Joint account holder or authorised persons can each register a unique PayID for the account.

9.2.9. The PayID Service does not support duplicate PayIDs. If you try to register a PayID for your account which is identical to another PayID in the service, you will see an error message. You can contact us to discuss duplicate PayIDs by calling 02 4941 3888. We cannot disclose details of any personal information in connection with duplicate PayIDs.

9.2.10. We will ensure that your PayID and account details are accurately recorded in the PayID Service.

9.3 Changes to your PayID

9.3.1. You must notify us immediately if you are no longer authorised to use a PayID or your details change. Please call us on 02 4941 3888.

9.4 Transferring your PayID to another account with Hunter United

9.4.1. You can transfer your PayID to another account with us by submitting a request to change your linked account using Internet Banking.
9.4.2. A transfer of your PayID to another account with us will generally be effective immediately, unless we notify you otherwise.
9.4.3. Deregistered (Closed) or Disabled (locked) PayIDs cannot be transferred. See below for information on Disabled (locked) PayIDs.

9.5 Porting (transferring) your PayID to an account with another Financial Institution

9.5.1. You can transfer your PayID to an account with another financial institution by submitting a request to port your PayID using Internet Banking.
9.5.2. A port (transfer) of your PayID to another financial institution is a two-step process initiated by you and completed by that financial institution. First, submit your port (transfer) request via our Internet Banking which will place your PayID into a porting (transfer) state and then complete the transfer via your new financial institution.
9.5.3. Until the transfer is completed, payments to your PayID will be directed to your account with us. If the other financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain with your account with us.

9.6 Porting (transferring) your PayID from another Financial Institution to your Hunter United account

9.6.1. To port (transfer) a PayID that you created for an account with another financial institution to your account with us, you will need to start the process with that financial institution and then you will need to register (create) that PayID with us. See above for more information on registering your PayID.

9.7 Deregistering (closing) a PayID

9.7.1. You can close your PayID by submitting a request to deregister your PayID using Internet Banking.
9.7.2. You must notify us immediately if you no longer own or have authority to use your PayID.
9.7.3. We may deregister (close) your PayID where:
(a) we are not satisfied that you are authorised to use your PayID;
(b) we reasonably suspect that the PayID has been used for a fraudulent purpose;
(c) the linked account for that PayID is closed;
(d) the PayID has been inactive for a period that we reasonable consider to be excessive; or
(e) we are required by law or by the operator of the NPP.
9.7.4. Deregistering of your PayID will generally be effective immediately if initiated by you through Internet Banking. If initiated through other channels we will deregister the PayID within one business day.

9.8 Disabling (locking) a PayID

9.8.1. We monitor PayID use to manage PayID misuse and fraud. You acknowledge and consent to us disabling (locking) your PayID if we reasonably suspect misuse of your PayID or use of your PayID to procure payments fraudulently.
9.8.2. Request to enable (unlock) a Disabled (locked) PayID may be made by calling us on 02 4941 3888.
9.8.3. While your PayID is Disabled you will not be able to make any changes to your PayID or receive NPP Payments to that PayID.

9.9 PayID Privacy

9.9.1. By registering your PayID you acknowledge that:
(a) You authorise us to record your PayID, PayID Name and account details (including full legal account name) ('PayID Record') in the PayID Service;

(b) You authorise payers' financial institutions to use your PayID information for the purposes of constructing payment messages, enabling payers to make payments to you, and to disclose your PayID Name to payers for payment validation.

(c) To the extent that the creation and use of the PayID Record constitutes a disclosure, storage and use of your personal information within the meaning of the Privacy Law, you acknowledge and agree that you consent to that disclosure, storage and use.

SECTION 10 – Osko

Our Osko Facility is available via Internet Banking (including Mobile Phone Banking and Touchscreen Teller) and allows you to send and receive payments in near-real time 24 hours a day using the New Payments Platform (NPP). This section applies if your account permits the use of the Osko Facility. Consult your account's *Product Key Fact Sheet* or terms and conditions to see if this Account Access Facility is available on your account

10.1 Osko General Terms

10.1.1. Osko is a payment service that allows you to send and receive payments in near-real time, 24 hours a day using the New Payments Platform (NPP).
10.1.2. Hunter United subscribes to Osko under the BPAY Scheme.
10.1.3. The Osko service we provide allows you to make and receive Osko Payments in near real-time.
10.1.4. We will tell you if, for any reason, we are no longer able to offer you Osko.
10.1.5. If we are no longer able to offer you Osko, you will not be able to send or receive Osko Payments through us.
10.1.6. Where we are able to do so we will tell you:
(a) if there are any delays in processing transactions;
(b) when your transaction is likely to be completed; and
(c) give you the opportunity to cancel a transaction if it is delayed.
10.1.7. Delays may occur in processing Osko Payments where:
(d) we delay processing to investigate and review the transaction to ensure it is not fraudulent or suspicious;
(e) we delay processing to comply with any applicable laws (including any laws relating to sanctions or anti-money laundering); or
(f) the recipient's financial institution delays processing.
10.1.8. It may take up to one business day for the Osko Facility to be available to new accounts.

10.2 Receiving an Osko Payment

10.2.1. You will receive an Osko Payment if:
(a) Your accounts terms and conditions permit the use of the Osko Facility. Consult your account's Product Key Fact Sheet or terms and conditions to confirm;
(b) we and the payee's financial institution and account support Osko; and
(c) if the payment is addressed to your PayID, that PayID is not Disabled or Deregistered.
10.2.2. You will need to use Internet Banking to view full remittance details of Osko Payments.
10.2.3. Joint account holders or authorised persons on your account may be able to see messages and notifications associated with payments addressed to your PayID.

10.3 Making an Osko Payment

10.3.1. You can make an Osko Payment through our Internet Banking Facility.
10.3.2. You will be able to make an Osko Payment if:
(a) You are registered and have full access to our Internet Banking Facility;
(b) Your accounts terms and conditions permit the use of the Osko Facility. Consult your account's Product Key Fact Sheet or terms and conditions to confirm;
(c) we and the recipient's financial institution and account support Osko; and
(d) if the payment is addressed to a PayID, that PayID is not Disabled or Deregistered.
10.3.3. You do not have to have a registered PayID to make an Osko Payment.
10.3.4. You can make an Osko Payment to a PayID or BSB and account number, provided that the payees' financial Institution and account support Osko.
10.3.5. We will treat your instruction to make an Osko Payment as valid if:
(a) You provide the amount of the payment;
(b) You provide the recipients PayID or BSB and account number; and

(c) when you give such information to us you comply with the security procedures specified in clause 4.2.

10.3.6. We will debit the account you specified with the amount of that Osko Payment when it is confirmed.

10.3.7. We are not obliged to make an Osko Payment if:

(a) You do not give us all of the above information or if it is inaccurate;

(b) We reasonably consider the transaction to be fraudulent;

(c) The payment description contains offensive material; or

(d) It poses a risk to the systems or integrity of Hunter United, the NPP or Osko.

10.3.8. You should ensure that all information you provide in relation to an Osko Payment is correct as we will not be able to cancel an Osko Payment once it has been processed.

10.3.9. When you enter the PayID into the payee field we will verify if the PayID has been registered into the PayID Service and display the payee's PayID Name to you. You must check that the PayID Name is who you intend to pay. If you make a payment to the wrong PayID you make not be able to recover your funds. See Mistaken Internet Payments clause 2.4.

10.3.10. When you direct an Osko Payment to a PayID connected to a joint account, other account holders may be able to see the messages and notifications associated with the payment.

10.3.11. In order to better provide you with the services under Osko, we may retain certain information relating to PayIDs you use. For example, we may retain information relating to PayIDs you provide us in order to facilitate scheduled payments (when available). See our Privacy Policy on our website for more information on how we collect, use, handle and store personal information.

10.3.12. You must comply with the terms and conditions applying to the account to which you request us to credit or debit an Osko Payment, to the extent that those account terms are not inconsistent with or expressly overridden by these terms. These terms are in addition to those terms.

10.3.13. If there is any inconsistency between the terms and conditions applying to the relevant account and/or service and these terms, these terms will apply to the extent of that inconsistency.

10.4 Transaction limits

10.4.1. A $1,000 limit per transaction will apply to payments you make using Osko.

10.4.2. A $5,000 daily limit will apply to payments you make using Osko. For example, you may make five $1,000 Osko payments before reaching your limit.

10.4.3. Osko transactions are included toward your daily Internet Banking transaction limit as described in clause 4.2.

10.4.4. You may apply to amend (increase or decrease) your NPP transaction limit and NPP daily limit. Please contact us for more information on how to do this. We may on reasonable grounds refuse to increase the limits.

10.4.5. We may reduce the limits applying to your account at any time if we consider it reasonably necessary to protect us or you.

10.5 Mistaken and Misdirected Osko Payments

10.5.1. You are solely responsible for providing correct payment details including amount and payee details.

10.5.2. Mistaken Internet Payments and Misdirected Payments will be dealt with in accordance with clause 2.4 above.

10.6 Suspension and termination

10.6.1. We may make the Osko service temporarily unavailable for the purpose of performing system maintenance or upgrades

10.6.2. We may suspend or terminate your Osko Facility if:

(a) we suspect that you, or someone acting on your behalf, is being fraudulent;

(b) we suspect that you are using Osko in a manner that will or is likely to affect our ability to continue providing Osko to you or our other customers; or

(c) you breach any obligation under these terms.

10.6.3. We may immediately terminate and/or suspend your Osko Facility by notifying you if our membership to the BPAY Scheme or our subscription to Osko is suspended, ceases or is cancelled (as the case may be) for any reason.

10.6.4. Termination or suspension of your right to use Osko does not:

(a) prejudice any claims either party may have against the other in respect of any then subsisting breaches of these terms; or

(b) otherwise affect the accrued rights or remedies of either party.

10.7 Privacy and confidentiality

10.7.1. In order to provide you with services under Osko, we may need to disclose your personal information to BPAY and/or its Service Providers. If we do not disclose your personal information to BPAY or its Service Providers, we will not be able to provide you with services under Osko. Accordingly, you agree to our disclosing to BPAY, its Service Providers and such other participants involved in Osko such personal Information relating to you as is necessary to facilitate the provision of Osko to you.