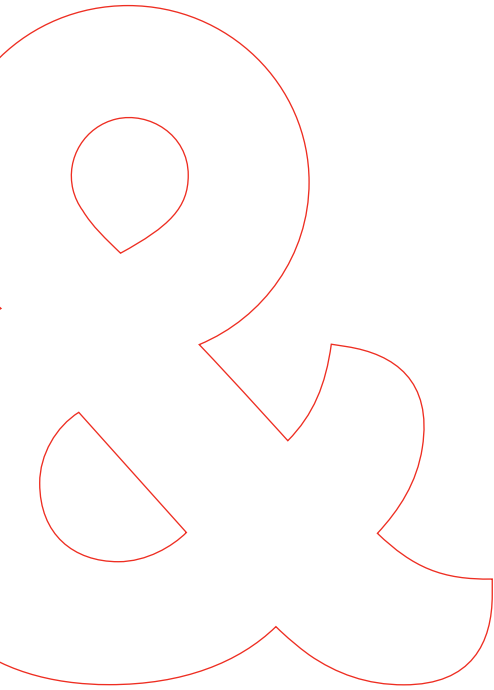
Credit Card

Account Access Conditions of Use

Effective from 19 October 2023



p&n bank

These Account Access Conditions of Use set out the terms that apply to the use of a Card, Online Banking Services and Phone Banking and the P&N Bank Mobile Banking App to access your Account.

NB: This booklet does not contain all the information we are required to give you before you enter a credit contract. Other information is contained in the Schedule and the Credit Card Conditions of Use.

Please read each of these documents carefully and ensure that any Additional Cardholder does likewise.
A copy of these documents should be kept for your future reference.

To report a lost or stolen Card, phone 13 25 77

Contents

Part 1 - General Terms

1. Interpretation

What some important words mean

1.1 In addition to the defined terms in the Credit Card Conditions of Use, the following defined terms apply to these Account Access Conditions of Use:

Access Code means the Access Method required by a User along with a member number, to access Online Banking Services and Phone Banking. The Access Code is chosen by the User but must meet our requirements as advised from time to time.

Access Method means a method authorised by us for use by a User as authority to process transactions, make BPAY® payments and permit access to your Account and includes, but is not limited to, any one of and any combination of, a Card, Card Details, member number, account number, Access Code, SMS Code and PIN, but does not include a method which requires your manual signature.

Biller means an organisation which tells you that you can make bill payments to them through the BPAY® Scheme.

BPAY® payment means a payment to a Biller through the BPAY® Scheme.

BPAY® Pty Ltd means BPAY® Pty Ltd ABN 69 079 137 518, PO Box 3545 Rhodes NSW 2138.
Tel: (02) 9646 9222.

BPAY® Scheme means a service which allows you to make BPAY® payments electronically to Billers. We are a member of the BPAY® Scheme. We will tell you if we cease to be a member of the BPAY® Scheme.

Card means a Physical Card or a Digital Card (as the case may be).

Chargeback means a transaction (other than a BPAY® payment) that, in accordance with the Credit Card Scheme Rules, is returned to a Merchant for resolution and reversal after it is disputed by a User.

Credit Card Scheme Rules means the credit card rules of Visa.

Digital Card means a digital Visa Credit Card we issue to you or to any Additional Cardholder to access your Account.

Digital Wallet means a mobile application which enables a User to make transactions using their Card or Card Details through a Device, including contactless payments at an electronic funds transfer point of sale terminal and online purchases.

Digital Wallet Provider means the person operating a Digital Wallet, for example, Google (for Android Pay).

EFTPOS Terminal means an electronic funds transfer point of sale terminal.

EFT System means the shared system under which EFT Transactions are processed.

EFT Terminal means any terminal connected to the electronic banking system and authorised by us for use with an Access Method to conduct an EFT Transaction, including ATMs and EFTPOS Terminals.

EFT Transaction means an electronic funds transfer initiated by giving an instruction to us through Electronic Equipment and using the Card (with or without a PIN), or Card Details (including through a Digital Wallet), but not requiring a manual signature.

Electronic Equipment means, but is not limited to, an EFT Terminal, computer, television, telephone, mobile telephone or any other small screen device which can be used to access the internet.

Funds Transfer means a service available through Online Banking Services and Phone Banking that allows a User to transfer funds from the Account to another account, held by you or another person with us or another financial institution.

Linked Account means an account other than the Account, nominated by you that we authorise you to access using your Card.

Mistaken Internet Payment means a Funds Transfer transaction from your Account initiated through Online Banking Services and Phone Banking where funds are paid into the account of an unintended recipient held with a financial institution that is a subscriber to the ePayments Code because the wrong BSB number and/or account number or other identifier was entered. This does not include payments made through BPAY® or Funds Transfer transactions made through Phone Banking Services.

Online Banking Services means the services we provide through Internet Banking and the P&N Bank

Mobile Banking App that may allow a member to access certain information about their account, change their personal details or preferences. or perform a range of transactions.

P&N Bank Mobile Banking App means a mobile phone banking service that allows a User to access certain information about their Account and perform a range of transactions through a software application installed on a mobile phone or tablet computer. The software can be downloaded through the App Store (for Apple Devices) or Google Play (for Android Devices).

Participating Online Merchant means a Merchant who offers goods or services for sale online, who is a participant in Visa Secure.

Visa payWave* means the functionality on specific Visa Cards that enables you to make small value Purchases at participating Merchant outlets without use of a PIN.

Phone Banking means our telephone banking system through which Users can access certain information about, and perform certain transactions in respect of the Account.

Physical Card means a physical Visa Credit Card we issue to you or to any Additional Cardholder to access your Account.

PIN means the personal identification number we allocate to a User for use with a Card as changed by you or us from time to time.

Secret Code means individually and collectively a User's PIN, Access Code, answers to Secret Questions, SMS Code, or any other password or secret code required to confirm a transaction or User, including a smartphone or tablet passcode, each of which the User must keep secret.

Secret Questions means security questions pre-arranged with us that may be asked when you wish to perform certain transactions or use certain functions in Online Banking Services and Phone Banking. The correct answers must be provided before the transactions can be made or the functions used.

SMS Code means a randomly generated 6 digit code we send by short messaging service (SMS) to your mobile phone for you to perform certain transactions

or use certain functions in Online Banking Services and Phone Banking and which, when requested, you must correctly enter in addition to your member number and relevant Access Code.

Unauthorised means without the knowledge or consent of a User.

Visa Secure* means the online transaction authentication service provided by us (or our nominated service provider).

* Visa payWave, Visa Secure and Visa are trademarks owned by Visa international Service Association and used under licence.

2. When we can change your Contract and how we will tell you?

2.1 We may change these Credit Card Account Access Conditions of Use at anytime as set out in this clause 2, for one or more of the following reasons:

(a) to comply with any change or anticipated change in any relevant law, code of practice, guidance or general banking practice;

(b) to reflect any decision of a court, ombudsman or regulator;

(c) to reflect a change in our systems or procedures, including for security reasons;

(d) to respond to changes in the cost of providing credit (including by changing interest rates);

(e) to discontinue a product in which case we may change the terms of your product to reflect a different product with similar features to the discontinued product; or

(f) to make the Contract clearer or to add features;

but will only do so in order to protect our legitimate business interests, and only to the extent reasonably required to do this.

2.2 We will give you at least 20 days' prior notice (or such long period required by law) by writing (which may be provided with or on your statement) of of any change that:

(a) imposes or increases fees or charges relating solely to the use of an Access Method or the issue or use of any additional or replacement Access Method;

(b) increases your liability for losses relating to transactions; or

(c) imposes, removes or adjusts a daily or periodic transaction limit applying to use of an Access Method.

2.3 We will give you notice of any changes to these Credit Card Account Access Conditions of Use that relate to the use of Digital Wallets before the change takes effect, by advertisement in the national or local media, notice in a newsletter or statement of account, individual notice sent to you in writing, by email, by SMS or by sending you a message through internet banking or the P&N Bank Mobile Banking App.

2.4 We will notify you of any other changes to these Credit Card Account Access Conditions of Use no later than the day the change takes effect, or such longer period as may be required by law, by:

(a) notices on or with your statements;

(b) direct written notice to you (which may be provided with or on your statement); or

(c) publishing changes on our website pnbank.com.au,

except where the change is adverse to you in which case we will notify you at least 30 days before the effective date of the change by advertisement in the national or local media or in writing (which may be provided with or on your statement).

2.5 We are not obliged to give you advance notice if an immediate change to these Credit Card Account Access Conditions of Use is deemed necessary for the security of our systems or individual accounts.

2.6 If you are unhappy with the changes we have made to these Credit Card Account Access Conditions of Use, you can cancel your Card.

3. Linked Accounts

3.1 If we allow your Card to be used to access a Linked Account, use of your Card in this way will be subject to the Visa Debit Card Terms & Conditions as if it was a 'Card' for the purposes of those terms and conditions. Any other terms and conditions applicable to your Linked Account will also apply. A copy of these terms and conditions are available at www.pnbank.com.au or by calling us on 13 25 77. Additional Cardholders will not be able to access your Linked Account through their Card unless they are authorised as a signatory to your Linked Account.

3.2 Except for this clause 3.2 and clause 11.1, the terms of this Contract will not apply to the Use of your Card to access a Linked Account. To access a Linked Account with the Card at an ATM or EFTPOS Terminal, select 'Debit' or 'DR' and not 'Credit' or 'CR'.

Please Note! If your Card gives you access to a Linked Account and your Card is cancelled in accordance with clause 10.1 of the Credit Card Conditions of Use, you will no longer be able to access the Linked Account through your Card.

4. Electronic Communications

4.1 You may opt-in to receive communications (including statements) electronically through Online Banking Services. If you do, we may make communications, including your statements, available for you to review in Internet Banking. We will send to you an email to tell you when you have a new statement to view.

4.2 If you do opt-in to receive electronic communications we may no longer send you physical communications. You should check your emails regularly to see if we have sent you anything. You can withdraw your consent at any time.

Part 2 - Use of the Card

5. Purpose of use

5.1 A User must use their Card (or Card Details) for personal, domestic or household purposes only. We reserve the right to determine, acting reasonably, whether a User's use, or proposed use, of a Card is in accordance with this requirement.

5.2 A User must not use a Card (or Card Details) for an unlawful purpose, including but not limited to the Purchase of any goods or services prohibited by Australian law, or the law of any jurisdiction in which a Card (or Card Details) is used or the goods or services are provided.

5.3 You authorise us to act on any instructions given by a User (for example, when a User initiates a transaction from an EFT Terminal using their Card).

6. Using the Card at Merchants

6.1 Cards can be used in Australia and most other overseas countries.

6.2 Users can use their Cards at Merchants displaying the Visa Card symbol and which accept the Card. If a User is using a Card at a Merchant in Australia that User may be required to swipe or insert their Physical Card into an EFTPOS Terminal and to select 'Credit' or 'CR'. The User will also generally be required to enter their PIN or may be required to sign a voucher to authorise the transaction.

6.3 If the User's card is Visa payWave enabled, or the User has registered the Card with a Digital Wallet, the User can instead make a transaction by holding their Card or their Device against a contactless reader enabled EFTPOS Terminal. Payments using Visa payWave or a Digital Wallet can only be made at participating Merchants.

Visa payWave may only be used for Purchases under a specified amount. If the Purchase is equal to or over the specified amount, the User will generally be required to authorise the transaction in the way specified in clause 6.2. Both the Visa and our own security systems continue to protect from Unauthorised Transactions using the Visa payWave process. However, we cannot guarantee the functionality of Visa payWave as it is provided by third parties. On this basis, we do not accept any liability for any interruption or malfunction of Visa payWave for any reason.

6.4 A User must check the transaction details entered into the EFT Terminal to ensure that they are correct, before authorising a transaction. The User should also check the completed transaction to ensure that it has been processed according to the User's instructions.

6.5 A Merchant may obtain an authorisation for payment of services or goods before a transaction is made to ensure that you have sufficient funds for the transaction (e.g. if a User pre-books a room in a hotel, the hotel may check that there are sufficient funds in the Account to pay for the room). Once this authorisation is completed, the amount of available credit in your Account will be reduced. If the transaction is not completed following the authorisation, the amount debited to your Account may not be returned to your Account for up to 6 Business Days.

6.6 If a Merchant accepts payment with a Card by mail order, telephone or online, Users may authorise payment in the manner required by the Merchant, usually by providing the Card Details.

6.7 The Visa Secure service may apply to online transactions made at participating merchants. Visa Secure is a service designed to provide improved security when a Card is used through the internet.

6.8 Users can also use their Card to pay the bills of water, gas, power and other utility suppliers. Unless the payment is made through BPAY®, it can be completed like any other transaction made at a Merchant. BPAY® payments are subject to clause 17 of these Account Access Conditions of Use.

7. Using the Card at ATMs or other financial institutions

7.1 Users can use their Card in combination with their PIN to obtain a Cash Advances at ATMs displaying the appropriate symbol in Australia and most other countries.

7.2 The minimum cash advance you can obtain at an ATM is the smallest denomination of notes available at that ATM. In Australia, this is generally $20 or $50 depending on the ATM. A User can also obtain a Cash Advance at a P&N Bank branch or the branch of another financial institution displaying the Visa card symbol located in Australia or overseas. A cash advance cannot be obtained through an EFTPOS Terminal.

7.3 If a User obtains a Cash Advance or makes a balance enquiry at an ATM, the ATM owner may charge a fee. In Australia, in relation to ATMs, this fee will be disclosed at the time of the transaction. Such fees will be debited to your Account if you choose to proceed.

8. Digital Wallets

8.1 Users may use a Digital Wallet to make contactless payments using their Card through a compatible Device. This clause 8 sets out the particular terms that apply to the use of a Card in a Digital Wallet.

8.2 There may be additional terms and conditions imposed by the Digital Wallet Provider, or the provider of a Device or telecommunications service, and Users are also required to comply with them.

8.3 A User's ability to register a Card into a Digital Wallet is at our reasonable discretion. We will provide reasons if we will not or cannot register a Card into a Digital Wallet.

8.4 We do not guarantee that any or all Merchants will accept payment using the Digital Wallet. We are not liable for any loss or inconvenience incurred as a result of the refusal of any Merchant to accept payment in this way.

8.5 We are not the provider of the Digital Wallet, and are not responsible for its use or function, including any disruption, failure, malfunction or unavailability or any security breach affecting information stored in or sent from the Digital Wallet, except to the extent that the loss is caused by our fraud, negligence, or wilful misconduct (including that of our officers, employees, contractors or agents). Users should contact the Digital Wallet Provider if they have questions or concerns about the Digital Wallet.

8.6 If you access a Device using biometric recognition, such as a fingerprint, no Secret Codes will be required in order for you to make payments through the Digital Wallet on that Device. To protect your Account, you should ensure that:

(a) only your biometrics are stored in that Device; and

(b) that Device, and your biometrics used in connection with that Device, remain secure at all times.

8.7 We do not charge any fees for the use of a Digital Wallet in addition to the fees and charges that already apply to the use of a Card. Third party fees and charges may apply to the use of a Digital Wallet, such as those imposed by a telecommunications service for data usage and text messaging.

8.8 We can suspend or cancel the ability to use a Card to make payments using a Digital Wallet. We may do so reasonably and at any time in order to protect our legitimate business interests, for example, if we reasonably suspect fraud with the Card, if you are in default under the Contract, if applicable laws change, if we cease to permit Cards to be used with any Digital Wallet, or if we are directed to do so by the Digital Wallet Provider or the applicable card scheme. We will notify you if we do so.

8.9 A User may remove a Card from a Digital Wallet at any time by following the Digital Wallet Provider's procedures for removal.

8.10 A User's Device may be linked to other Devices by a common account. If so, when a Card is added to a Digital Wallet using the Device, that Card may also be accessible through a Digital Wallet on a linked Device, which may permit users of the linked Device to see the Card Details and make payments with that Card.

9. Some Merchants may charge a surcharge

Once you have completed a transaction you will not be able to dispute the surcharge. Our liability for Merchants or other financial institutions is limited.

9.1 To the extent permitted by law, we do not accept responsibility for the actions of other financial institutions or Merchants:

(a) in refusing to accept or honour a Card; or

(b) in imposing limits or conditions on use of a Card.

Users must resolve such issues directly with the financial institution or Merchant.

9.2 Card promotional material displayed at any Merchant's premises does not mean that all goods and services at those premises may be purchased using a Card.

9.3 Unless required by law, we are not responsible for goods or services supplied to a User or for any refund. The User must take up any complaints or concerns directly with the Merchant and any refund is a matter between the User and the Merchant. If a Merchant gives the User a refund we will only credit the Account when we receive correctly completed refund instructions from the Merchant. If a refund is received from an overseas Merchant, there may be a difference in the Australian dollar values of the item at the time of the Purchase and refund due to fluctuations in currency exchange rates. You take the risk of the fluctuation.

10. Do transactions have to be authorised by us?

10.1 At times, transactions on your Account may need to be authorised by us. We also may, at our reasonable discretion, decline to authorise any transaction on your Account (e.g. for security reasons or if your Credit Limit would be exceeded).

10.2 We are not liable to you or to any third party for any damage resulting from our refusal to authorise a transaction and you indemnify us in respect of any such loss, except to the extent that the loss is caused by our fraud, negligence or wilful misconduct (including that of our officers, employees, contractors or agents), or as otherwise provided by these Account Access Conditions of Use.

10.3 If we authorise the transaction, the amount of available funds in your Card Account will be reduced according to the amount of the transaction. If the User, or the Merchant, fails to proceed with the transaction after it has been authorised by us, the amount of available credit in your Account may be reduced for up to 6 Business Days.

11. Transaction limits

11.1 A maximum Cash Advance limit may apply to your Account (and may be zero). If so, the Cash Advance limit will be the amount we may authorise from time to time. The Cash Advance limit we determine is at our reasonable discretion. However, we will take into account things such as our credit risk assessment of you, the period for which the Account has been operated and your payment history.

11.2 The total amount of Funds Transfer transactions that can be made from all accounts you hold with us is $5,000 a day (including your Account and any Linked Accounts), unless we otherwise agree.

11.3 BPAY® payments from all accounts you hold with us cannot exceed AU$10,000 a day (including your Account and any Linked Accounts), unless we otherwise agree.

11.4 We may, at any time, acting reasonably, limit the number or value of EFT Transactions which may be undertaken by Users, including on a periodic basis. We may at any time change any such limit. If we remove or increase such a limit, this may increase your liability in the case of Unauthorised Transactions.

11.5 Additional restrictions may be imposed by Merchants and other financial institutions.

12. Regular payment arrangements

12.1 Users may authorise a Merchant to charge amounts to your Account on a regular basis by

giving them their Card Details. If they do, they should make a record of any authority given or payment arrangement made (including, a record of the Merchant's name, contact details, amounts and dates upon which payments will be processed).

12.2 If a User wishes to cancel or change a payment authority or arrangement, the User should notify the Merchant in writing at least 15 Business Days before the next payment is due and should make and keep a copy of any request sent to the Merchant. Until the Merchant is notified, we are required to process the regular payments to the Merchant. However, if the Merchant fails to comply with a request to cancel the authority or arrangement, you can dispute any charges (see clause 29 'Chargebacks' of these Account Access Conditions of Use).

12.3 If a User's Card Details change because a new or replacement Card is issued (for example, if a Card is lost or stolen or if you have requested a Card Contract Variation), the User should provide the new details to any relevant Merchant to ensure the continuation of any regular payment arrangement and the continued provision of the relevant goods or services.

12.4 Should your Account be closed or access to the Account suspended, by you or us, you should contact all Merchants with whom any User has a regular payment arrangement and advise them of any new arrangement you may wish to make in order to avoid disruption to the goods or services supplied by the Merchant.

13. What happens if the Card is used overseas?

13.1 You are liable for the Australian dollar equivalent of the amount of all overseas transactions authorised by a User.

13.2 All transactions made in foreign currency on your Card will be converted into Australian currency by Visa. The exchange rate used will be selected by Visa from the range of rates available in wholesale currency markets on the processing date, or the government mandated rate that is in effect at that time. For these conversions a charge that is made in United States dollars, Canadian dollars, New Zealand dollars, Singapore dollars, pounds

sterling, euros and Japanese yen is converted directly into Australian dollars. A charge that is made in any other foreign currency is converted into United States dollars before being converted into Australian dollars.

13.3 Transactions may not be processed to your Account on the same day that they occur. To the extent permitted by law, you bear the risk of a change in exchange rates in the intervening period.

13.4 Some overseas Merchants and EFT Terminals charge a surcharge for undertaking an EFT Transaction. Once you have completed the transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement of account as part of the purchase price of such transaction.

13.5 Before travelling overseas, Users should consult us to obtain the Visa Credit Card Hotline number for their country of destination. Users should use the Visa Credit Card Hotline if any of the circumstances described in clause 20.1 occur.

13.6 Users must comply with all applicable exchange control and tax laws governing the use of their Card and you indemnify us against liability, loss, fees, charges or costs arising as a consequence of a failure to comply with them.

13.7 For all transactions occurring outside Australia, we will charge the foreign currency conversion fee described in the Schedule or notified by us from time to time.

Part 3 - Online Banking Services and Phone Banking

14. Access to Online Banking Services

14.1 Depending on the functionality of the services you are using, Internet Banking and the P&N Bank Mobile Banking App can be used to access information about your account, change your personal details or preferences, or make a range of transactions 24 hours a day. (External transfers made during business hours may be processed immediately. All others may be processed the next business day.)

14.2 You must apply for each Online Banking Service separately.

14.3 Separate Terms & Conditions apply to your use of Online Banking Services (including Bpay). These

Terms & Conditions will be provided to you at the time of application. You can also obtain a copy on our website pnbank.com.au or by contacting us. You should read these Terms and Conditions carefully before using Online Banking Services.

14.4 To the extent of any inconsistency between these Terms & Conditions and the Online Banking Services Terms and Conditions, the Online Banking Services Terms and Conditions will prevail.

15. Mistaken Internet Payments

15.1 If you have made a Mistaken Internet Payment, you can report it to us by:

(a) on 13 25 77 and providing us with the details of the Mistaken Internet Payment; or

(b) completing a Mistaken Internet Payment Form available at pnbank.com.au and sending it to P&N.

If you make a report to P&N that a payment made from your account to an external bank account was a Mistaken Internet Payment:

within 10 business days of making the payment, and there are sufficient credit funds available in the account of the unintended recipient, and both P&N and the other financial institution (at which the relevant account to which the Mistaken Internet Payment was made is held) are satisfied that a Mistaken Internet Payment occurred, then the other financial institution must return the funds to P&N Bank within 5 to 10 business days of receiving a request. P&N Bank will then return the funds to you as soon as practicable.

between 10 business days and 7 months of making the payment, and there are sufficient credit funds available in the account of the unintended recipient and P&N is satisfied that a Mistaken Internet Payment occurred, then the other financial institution must complete its investigation within 10 business days of receiving a request. If, after completing its investigation, the other financial institution is satisfied that a Mistaken Internet Payment occurred, it must prevent the unintended recipient from withdrawing the funds mistakenly paid for 10 further business days. The other financial institution must notify the unintended recipient that it will withdraw funds in the amount of the Mistaken Internet Payment if the unintended recipient does not establish that they are entitled to the funds within 10 business days. If the unintended recipient does not establish that they are entitled to the funds within 10 business days, the other

financial institution must return the funds to P&N within a further 2 business days. P&N will then return the funds to you as soon as practicable.

after 7 months of making the payment, and there are sufficient credit funds available in the account of the unintended recipient, and both P&N and the other financial institution are satisfied that a Mistaken Internet Payment occurred, then the other financial institution must seek the consent o the unintended recipient to return the funds mistakenly paid. If the unintended recipient consents to the return of funds, the other financial institution must return the funds to P&N. P&N will then return the funds to you as soon as practicable.

at any time and P&N is satisfied that a Mistaken Internet Payment occurred but the other financial institution is not satisfied that a Mistaken Internet Payment occurred and there are sufficient credit funds available in the account of the unintended recipient, the other financial institution may seek the consent of the unintended recipient to return the funds mistakenly paid. If the unintended recipient consents to the return of the funds, the other financial institution must return the funds to P&N Bank and P&N Bank will return the funds to you as soon as practicable.

at any time and both P&N and the other financial institution are satisfied that a Mistaken Internet Payment occurred but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the Mistaken Internet Payment, the other financial institution must use reasonable endeavours to retrieve the funds mistakenly paid from the unintended recipient for return to you (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

at any time and P&N is not satisfied that a Mistaken Internet Payment occurred, P&N will not take any further action and you will be liable for the loss arising from the Mistaken Internet Payment. The other financial institution must notify the unintended recipient that it will withdraw funds in the amount of the Mistaken Internet Payment if the unintended recipient does not establish that they are entitled to the funds within 10 business days. If the unintended recipient does not establish that they are entitled to the funds within 10 business days, the other financial institution must return the funds to P&N within a further 2 business days. P&N will then return the funds to you as soon as practicable.

If you make a report to P&N that a payment made from your account to another bank account held with P&N was a Mistaken Internet Payment:

within 10 business days of making the payment, and there are sufficient credit funds available in the account of the unintended recipient, and P&N is satisfied that a Mistaken Internet Payment occurred, then we will return the funds to you within 5 to 10 business days of receiving your request.

between 10 business days and 7 months of making the payment, and there are sufficient credit funds available in the account of the unintended recipient and P&N is satisfied that a Mistaken Internet Payment occurred, then we will prevent the unintended recipient from withdrawing the funds mistakenly paid for 10 further business days. We must notify the unintended recipient that we will withdraw funds in the amount of the Mistaken Internet Payment if the unintended recipient does not establish that they are entitled to the funds within 10 business days. If the unintended recipient does not establish that they are entitled to the funds within 10 business days, we will return the funds to you within a further 2 business days.

after 7 months of making the payment, and there are sufficient credit funds available in the account of the unintended recipient, and P&N is satisfied that a Mistaken Internet Payment occurred, then we will seek the consent of the unintended recipient to return the funds mistakenly paid. If the unintended recipient consents to the return of funds, we will return the funds to you as soon as practicable.

at any time and P&N is satisfied that a Mistaken Internet Payment occurred but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the Mistaken Internet Payment, we will use reasonable endeavours to retrieve the funds mistakenly paid from the unintended recipient for return to you (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

at any time and P&N is not satisfied that a Mistaken Internet Payment occurred, P&N will not take any further action and you will be liable for the loss arising from the Mistaken Internet Payment.

- P&N will inform you of the outcome of a reported Mistaken Internet Payment in writing within 30 business days of the day on which the report is made.

- If you have a complaint about how your Mistaken Internet Payment report has been dealt with, you can make a complaint in accordance with clause 31.
- It is possible that you may receive a Mistaken Internet Payment into your account. If this occurs, we may be required to recover these funds and return the funds to the sender. P&N will notify you in writing if we do so. While we may, in some circumstances, seek your consent to return the funds, we will not always do so. In addition, there may be situations where you will need to prove your entitlement to the funds. If this occurs we will notify you in writing of the steps you need to take to confirm your entitlement to the funds.

16. Using Phone Banking

16.1 To use Phone Banking Users must call 13 25 77 and provide their member number and their Access Code. When a User performs a transaction using Phone Banking, you authorise us to act on the instruction of the User. Transactions will not necessarily be processed to the Account on the day they are performed.

16.2 We may refuse, at our reasonable discretion, to give effect to any instruction given by a User through Phone Banking and we will not be liable to you or any other person for any loss or damage which may be incurred or suffered as a result, except to the extent that the loss is caused by our fraud, negligence or wilful misconduct (including that of our officers, employees, contractors or agents).

16.3 Phone Banking cannot be used to effect transfers between accounts you hold with us if one of the accounts requires two or more signatures to operate the account. In that event, Phone Banking can only be used to obtain account information.

Part 4 - Using BPAY®

17. BPAY® payments

17.1 This section on "Using BPAY®" applies to BPAY® payments only. If there is any inconsistency between the provisions of this Part 4 "Using BPAY®" and the other provisions of these Credit Card Access Conditions of Use, the provisions of this Part 4 prevail.

17.2 Bill payments that are made through Online Banking Services and Phone Banking are processed through the BPAY® Scheme. Bills which may be paid through the scheme display the BPAY® logo and Biller reference details. Bills will also record the type of accounts from which the Biller will accept payment (e.g. cheque, savings or credit card).

17.3 The following information must be given to us to make a BPAY® payment:

(a) the Biller's code number (found on your bill);
(b) the User's customer reference number (e.g. the account number with the Biller);
(c) the amount to be paid;
(d) (if applicable) your Account details; and
(e) a date, if the payment is to be future dated.

17.4 We are not obliged to effect a BPAY® payment if the information given to us is inaccurate and/or incomplete or the payment would cause your Credit Limit or the daily BPAY® payment limit to be exceeded.

17.5 We will debit the value of each BPAY® payment to the Account and will treat it as a Purchase.

17.6 A BPAY® payment instruction is irrevocable. Except for future dated payments, we will not accept a request to stop a BPAY® payment once we have been instructed to make it.

17.7 Generally, a BPAY® payment is treated as received by the Biller to whom it is directed on the date we are told to make it if we receive the instruction by the cut off time of 1.30pm (Australian Western Standard time) on a Business Day. Otherwise, it is treated as received on the next Business Day after we receive the instruction. A BPAY® payment will therefore take longer to process if the payment instruction is given on a day which is not a Business Day.

17.8 A delay may occur in the processing of a BPAY® payment if a Biller or another financial institution participating in the BPAY® Scheme does not comply with its obligations under the BPAY® Scheme, or if there is a system malfunction.

17.9 If we are advised that a BPAY® payment cannot be processed by a Biller, we will advise you, will credit your Account with the amount of the BPAY® payment

and take all reasonable steps to assist you in making the BPAY® payment as quickly as possible.

17.10 Care must be taken by all Users to enter the correct amount to be paid to a Biller and to enter the correct Biller details. If the amount entered is greater than intended, the User must contact the Biller to obtain a refund of the excess. If less, a further BPAY® payment can be made for the difference. If the payment is made to a person other than the intended Biller and we cannot recover it from the recipient within 20 Business Days, you are liable for the payment amount.

17.11 You acknowledge 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 you and the Biller.

17.12 You should check your Account carefully and promptly report to us, as soon as you become aware of them, any BPAY® payments that you think are errors or were not authorised by a User. The longer the delay between the date of your BPAY® payment and when you tell us of the error, the more difficult it may be to correct the error. You may need to liaise directly with the Biller to correct the error if, for example, because of delay, we no longer have sufficient records to investigate it.

17.13 If a BPAY® payment is made by us to a person or for an amount which is not in accordance with the instructions given to us and your Account was debited with the payment, we will credit that payment amount to your Account.

17.14 If you tell us that a BPAY® payment made from your Account is unauthorised, you must give us your written consent addressed to the Biller who received that BPAY® payment, including your customer reference number and such information as we reasonably require to investigate the BPAY® payment. If you do not give us the consent, the Biller may not be permitted under law to disclose to us the information we need to investigate or rectify that BPAY® payment.

17.15 Disputes in relation to unauthorised, fraudulent or wrong BPAY® payments will be handled in accordance with clause 30 of these Account

Access Conditions of Use. Your liability for unauthorised and fraudulent BPAY® payments will be determined in accordance with clause 25 of these Account Access Conditions of Use. No Chargeback rights are available in respect of a BPAY® payment from your Account.

17.16 Subject to clause 25 of these Account Access Conditions of Use and the ePayments Code:

(a) we are not liable for any consequential loss or damage you may suffer as a result of using the BPAY® Scheme, other than due to any loss or damage you suffer due to our fraud, negligence or wilful misconduct (including that of our officers, employees, contractors or agents), or in relation to any breach of a condition or warranty implied by law under consumer protection legislation 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; and

(b) 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 did not observe any of your obligations under these Account Access Conditions of Use or acted negligently or fraudulently in connection with your use of, the BPAY® Scheme.

18. Future-dated BPAY® payments

18.1 Users may arrange BPAY® payments up to 60 days in advance of the time for payment.

18.2 We will not make the payment if, on the day(s) nominated for payment, the BPAY® payment will cause your Credit Limit or the daily BPAY® payment limit to be exceeded. In that event, it will be necessary for the User to resubmit the BPAY® payment instruction.

18.3 A future-dated BPAY® payment instruction may be altered or cancelled before the date stipulated for its payment, provided the instruction to alter or cancel the payment is given no later than on the Business Day immediately preceding the stipulated date.

Part 5 - Security of Access Methods

19. Guidelines to protect Access Methods

19.1 Users must protect relevant Access Methods at all times to prevent unauthorised access to your Account. They must take care to ensure that Access Methods are not misused, lost or stolen and that, where an Access Method is a Secret Code, the Secret Code does not become known to anyone else.

19.2 This clause contains guidelines which should be followed by Users to protect against unauthorised use of an Access Method. These guidelines provide examples only of security measures and will not determine your liability for losses resulting from any Unauthorised Transaction. Liability for Unauthorised Transactions will be determined in accordance with clause 25 of these Account Access Conditions of Use and the ePayments Code.

To protect a Physical Card:

- sign the Physical Card as soon as it is received;
- always keep the Physical Card in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- never lend the Physical Card to any person or permit any other person to use the Physical Card; and
- when a transaction is complete remember to take the Physical Card and the transaction receipt.

To protect a Digital Card:

- always keep your Device on, or account through, which your Digital Card can be viewed locked when you're not using it;
- never lend your Device on which your Digital Card can be viewed to any person or permit any other person to use your Device;
- if you use biometric recognition to access your Device on which your Digital Card can be viewed, ensure that only your biometrics are stored in your Device;
- ensure that your passcodes and biometrics stored in connection with your Device on

which your Digital Card can be viewed remain secure at all times; and

- log out from any account through which your Digital Card can be viewed when you are not using it.

To protect the Card Details:

- do not give or tell the Card Details to anyone; and
- use care to prevent anyone seeing the Card Details when entering them at Electronic Equipment.

To protect a Secret Code:

- where a Secret Code is issued by us, memorise the Secret Code when it is received and destroy our notice of the Secret Code;
- if given the option to select a Secret Code, Users should not select a Secret Code which represents a name, date, telephone number, car registration or anything else that could be associated with them, nor a Secret Code which has an easily retrievable combination (such as repeated numbers or letters);
- never tell or show a Secret Code to anyone, including a family member, friend or persons in authority (such as a bank officer or police officer);
- do not record a Secret Code on the Card or any Device;
- do not keep a record of the Secret Code (without making any reasonable attempt to disguise the Secret Code) with any article kept with the Card or any Device or which is liable to be lost or stolen simultaneously with the Card or any Device;
- do not record the Secret Code on a computer or telephone or on one or more articles likely to be stolen simultaneously without making a reasonable attempt to disguise the Secret Code;
- do not keep a Secret Code together with the Card or any Device, for example in a bag or wallet, in a car or in the same piece of furniture;
- do not keep a record of the Secret Code with any document containing the reference

numbers for the Card Account, such as statements;

- be careful to prevent anyone else from seeing the Secret Code being entered at Electronic Equipment and watch out for mirrors, security cameras or any means which enable other people to see the Secret Code being entered;
- do not access Online Banking Services and Phone Banking directly from a facility where the details entered may be recorded by a third party, for example, a hotel telephone or a computer at an internet café; and
- if a User suspects that someone else may know a Secret Code or that an unauthorised person is using a Secret Code, they should contact us immediately to request the issue of a new Secret Code.

We do not consider the following to be reasonable attempts to disguise a Secret Code:

- recording the disguised Secret Code on the Card or Device;
- disguising the Secret Code by reversing the number sequence;
- describing the disguised record as a Secret Code record;
- disguising the Secret Code as a telephone number where no other numbers are recorded;
- disguising the Secret Code as a telephone number, postcode, amount or date with the Secret Code in its correct sequence within the number;
- disguising the Secret Code using alphabetical characters, i.e. A=1, B=2, C=3 etc. or in any other easily understood code; or
- recording the Secret Code as a series of numbers or letters with any of them marked to indicate the Secret Code.

Users must not use any other form of disguise which is similarly unsuitable or such that another person can easily work it out.

Part 6 - Loss, theft or Unauthorised use of an Access Method

20. What Users must do

20.1 If any Card, or Device holding a Digital Wallet into which a Card has been registered or through which a Digital Card can be viewed, has been lost, stolen or used without authorisation, a Secret Code has become known to someone else, any security credentials on any Device are otherwise compromised, or you suspect that Unauthorised Transactions have been made on your Account (or a Linked Account), you or another User must immediately tell us by:

(a) calling;

- 13 25 77 (during business hours); or
- 1800 648 027 (the Visa Credit Card Hotline, which is available day or night, every day of the week); or

(b) sending us a notification through Internet Banking or our P&N Bank Mobile Banking App.

We will issue a reference number which should be kept as evidence of the time and date of the notification.

20.2 If the Visa Credit Card Hotline is not operating at the time notification is attempted, the loss, theft or Unauthorised use must be reported to us as soon as possible during business hours. We will be liable for any losses arising because the Visa Credit Card Hotline is not operating at the time of attempted notification, provided that the loss, theft or Unauthorised use is reported to us as soon as possible during business hours.

20.3 It is your responsibility to check your statement of account carefully as soon as you receive it and to notify us immediately of any errors or Unauthorised Transactions.

20.4 We recommend that you keep copies of any vouchers, dockets, receipts and transaction records (issued by us or anyone else) to enable you to check the accuracy of your statements of account.

21. What if a User is overseas?

If any of the events referred to in clause 20.1 occurs outside Australia, the User must confirm the loss, theft or misuse of the Card:

(a) with us, by telephone or priority paid mail, or through Online Banking Services or the P&N Bank Mobile Banking App, as soon as possible, or
(b) by telephoning the Visa Credit Card Hotline number for the country you are in, which you must obtain from us prior to your departure in accordance with clause 13 of these Account Access Conditions of Use.

22. Additional Card Controls

If any of the events referred to in clause 20.1 occur, you should immediately implement appropriate card controls (such as temporary card block), which you can do through Internet Banking or the P&N Bank Mobile Banking App.

What is your liability for Unauthorised EFT Transactions?

23. Your liability

23.1 The following clauses relate to your liability for EFT Transactions (including BPAY® payments) which are carried out without the knowledge or consent of a User (i.e. Unauthorised).

23.2 You are liable for all EFT Transactions carried out with the knowledge or consent of a User, regardless of when the transaction is processed to your Account with us, subject to any right we may have under the Credit Card Scheme Rules to request a reversal (i.e. "Chargeback") of the transaction for you (see clause 29).

24. You are not liable in the following circumstances

24.1 You are not liable for any loss arising from an Unauthorised EFT Transaction that occurs:

(a) where it is clear that the User has not contributed to the loss;
(b) by the fraudulent or negligent conduct of our employees or agents, or those of Merchants or any organisation involved in the EFT System.
(c) because any component of an Access Method is forged, faulty, expired, or cancelled;
(d) before the User has received their Card or Secret Code (as relevant);
(e) due to the same transaction being incorrectly debited more than once to the same account;
(f) after we receive notification that the User's Card, or Device holding a Digital Wallet or through which a Digital Card can be viewed, has been misused, lost or stolen or used without authority, or their Secret Code has become known to someone else;

(g) where the transaction is one which can be made using an identifier (i.e. a non-secret identifier such as your Account number) without a Secret Code (e.g. a PIN) or Card; or

(h) where the transaction is one which can be made using a Card, or a Card and an identifier (i.e. a non-secret identifier such as your Account number) but which, in either case, does not require a Secret Code, unless the User unreasonably delays reporting the loss or theft of the Card.

24.2 You are also not liable for any loss arising from any Unauthorised Transaction in an amount greater than the amount of your liability had we exercised our rights (if any) under the Credit Card Scheme Rules against other parties to that scheme, for example, Chargeback rights.

25. You are liable in the following circumstances

25.1 Subject to clause 25.2, you are liable for the loss arising from an Unauthorised Transaction that occurs before we receive notification that the User's Card or Device has been lost or stolen or used without authority or their Secret Code has become known to someone else and we prove on the balance of probability that the User has contributed to the loss by:

(a) the User's fraud;

(b) voluntarily disclosing their Secret Code to anyone, including a family member or friend;

(c) indicating a Secret Code on the Card, or keeping a record of a Secret Code (without making any reasonable attempt to protect the security of the record) on the one article, or on several articles, carried with the Card or any Device or liable to loss or theft simultaneously with the Card;

(d) where the Access Method comprises a Secret Code without a Card, keeping a record of a Secret Code (without making any reasonable attempt to protect the security of the code record) on the one article, or on several articles that are liable to loss or theft simultaneously;

(e) when changing a Secret Code, selecting a Secret Code which represents the User's

birth date or a recognisable part of the User's name;

(f) acting with extreme carelessness in failing to protect the security of the Secret Code;

(g) leaving a Physical Card in an ATM, as long as the machine incorporates reasonable safety standards that mitigate the risk of a card being left in a machine (for example, the machine captures cards that are not removed after a reasonable time or requires that the card be removed from the machine before the transaction can proceed); or

(h) unreasonably delaying notifying us of the Unauthorised use, theft or loss of the Card or any Device, or that the Secret Code has become known to someone else;

However, in the case of clause 25.1(h), you will only be liable for the losses which occur between when the User became aware of the loss, theft or unauthorised use (or should reasonably have become aware in the case of a lost or stolen Card or any Device) and when we were actually notified.

25.2 However, you will not be liable under clause 25.1 for:

(a) the portion of the loss on any day, or in any period, that exceeds any applicable daily or periodic transaction limit (as relevant);

(b) the portion of the loss on your Account which exceeds the Credit Limit of your Account;

(c) the portion of the loss on any Linked Account that exceeds the balance of the Linked Account; or

(d) any loss incurred on any account which you had not agreed with us could be accessed using the Access Method used to perform the transaction.

25.3 Where more than one Secret Code is required to a perform a transaction and we prove that the User breached the security of a Secret Code (by failing to comply with the requirements set out in clause 25.1) for one or more Secret Codes, but not all of the required Secret Codes, and we can prove on the balance of probability that the breach of security of the Secret Code(s) was more than 50% responsible for the losses when assessed together

with all the contributing causes, you will be liable in accordance with this clause 25.

25.4 Where a Secret Code was required to perform the Unauthorised EFT Transaction and clause 25.1 does not apply, your liability for any loss arising from an Unauthorised EFT Transaction, if the loss occurs before you notify us of the Unauthorised use, loss or theft of the Card or any Device, or of the Secret Code becoming known to someone else, is the lesser of:

(a) $150;

(b) the Credit Limit of your Account or the balance of your Linked Account (as relevant); or

(c) the actual loss at the time we are notified of the Unauthorised use, loss or theft of the Card or any Device or of the Secret Code becoming known to someone else (limited to any daily or periodic transaction limits applicable to the use of the Secret Code or account).

26. Liability for equipment malfunctions

26.1 You will not be responsible for any loss caused because the EFT System or EFT Equipment accepted a User's instructions but failed to complete the transaction.

26.2 If the User should reasonably have been aware that the EFT System or the EFT Equipment was unavailable for use or was malfunctioning our liability is limited to correcting any error in the Account and to the refund of any charges or fees imposed on you as a result.

27. Your maximum liability

27.1 Notwithstanding any of the provisions of clauses 24 and 26, your liability for Unauthorised EFT Transactions will not exceed your liability under the provisions of the ePayments Code, where that code applies.

What is your liability for other Unauthorised Transactions?

28. Your liability

28.1 If, in cases not involving EFT Transactions, a Card or Card Details are used without a User's authority, you are liable for the actual loss arising from the transaction at the time we are notified of the Unauthorised use (except that portion of

the loss incurred on any one day that exceeds any applicable daily transaction or other periodic transaction limit) less any amount recovered by us in the exercise of our rights (if any) under the Credit Card Scheme Rules against other parties to that scheme.

28.2 The provisions of the ePayments Code do not apply to your liability under this clause.

Chargebacks

29. How can you benefit from a Chargeback?

29.1 Under the Credit Card Scheme Rules we have the right in certain circumstances, and in respect of both authorised and Unauthorised Transactions, to seek, on your behalf, the reversal of a transaction (a "Chargeback") and its debiting to the Merchant's account with its financial institution. We may be entitled to do so, for example, where a User has effected a transaction by telephone with a Merchant and where the goods which were ordered and for which payment was made, were never delivered.

29.2 You should make every effort to report a disputed transaction to us in writing within 30 days of the date of the statement of account which itemises the disputed transaction, so that we may reasonably ask for a Chargeback where such right exists. A failure to report a disputed transaction, charge, refund or payment, and/or provide additional information within this timeframe and in the form we require could affect our ability to claim a Chargeback right (if any) under the Credit Card Scheme Rules.

29.3 If you dispute a transaction with us within the required timeframe and a Chargeback right exists under the Credit Card Scheme Rules, we will claim a Chargeback on your behalf without delay. We will also:

(a) ensure we claim the Chargeback for the most appropriate reason; and

(b) not accept a refusal to Chargeback by the Merchant's financial institution unless it is reasonable and consistent with the Credit Card Scheme Rules.

29.4 Where possible, we will assist you to seek a Chargeback of any Unauthorised Transaction debited to your Account under a regular payment arrangement where payments continue to be debited because the Merchant has not complied with a User's request to cancel the arrangement.

29.5 No Chargeback rights exist in relation to BPAY® payments (see clause 17.15).

Complaints, Disputes and their Resolution

30. Responding to your complaints

30.1 We are committed to responding to complaints and disputes in a way that is prompt and efficient, consistent with the law and applicable industry codes and in a manner that is fair to everyone involved. Our ability to deal effectively with any complaint a User may have will usually depend, however, on the User responding to our reasonable requests for information in respect of our consideration of the complaint.

30.2 If a User has a complaint (including about the service provided by us, an EFT Transaction (including an Unauthorised EFT Transaction) or a BPAY® payment the User can contact the nearest P&N Bank branch or call us on 13 25 77 to discuss the complaint.

30.3 If the complaint is not satisfactorily resolved during that discussion, we will refer the User to our Member Advocate, who will discuss the issue and attempt to resolve your complaint.

Name: Member Advocate
Mail: Police & Nurses
PO Box 8609
Perth BC,
Western Australia 6849
Ph: 13 25 77
Fax: (08) 9219 7660
Email: member.advocate@pnbank.com.au

30.4 If the dispute relates to an Unauthorised EFT Transaction, the User will need to complete an EFT Enquiry/Investigation Form and send it to us or otherwise provide the information sought by that form to us.

30.5 Within 21 days of receipt from the User of the details of their complaint, we will:

(a) complete our investigation and advise the User in writing of the results of our investigation; or

(b) advise the User in writing that we require further time to complete our investigation.

30.6 We will complete our investigation within 45 days of receiving a complaint unless there are exceptional circumstances (for example due to delays caused by foreign Merchants). In such circumstances, we will let the User know of the reasons for the delay and provide monthly updates on the progress of the investigation and its likely resolution date. (The User may nevertheless after 45 days take their complaint to our External Dispute Resolution Scheme (see clause 31) even if we are still considering the complaint).

30.7 When we complete our investigation, we will write to the User to advise of the outcome of our investigation and the reasons for that outcome with reference to these Account Access Conditions of Use and the ePayments Code.

30.8 If we find that an error was made and this may include errors that were not the subject of the complaint, we will make the appropriate adjustments to your Account including interest and charges (if any) and will advise you in writing of the amount of the adjustment.

30.9 If your dispute relates to an Unauthorised Transaction and we decide that you are liable for all or any part of a loss arising out of the Unauthorised Transaction, we will:

(a) give you copies of any documents or other evidence we relied upon in reaching to this decision; and

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

30.10 If we fail to observe these procedures or the requirements of the ePayments Code for handling disputes, allocating liability, or communicating the reasons of our decision, and our failure contributes to our decision or delays the resolution of the complaint, we may be liable, under the ePayments Code, for all or part of the amount of the disputed transaction.

30.11 If we decide to resolve the User's complaint by exercising our rights under the Credit Card Scheme Rules, different time limits to those set out above (in this clause 30) may apply. If so, we will inform the User in writing of those time limits and when the User can reasonably expect a decision. We will also suspend your obligation to pay any amount which is the subject of the complaint and any charge related to that amount until your complaint has been resolved.

31. External Dispute Resolution (EDR)

31.1 If a User is not satisfied with our decision in respect of a complaint, the User may contact our independent external dispute resolution scheme in respect of the complaint:

Name: The Australian Financial Complaints Authority (AFCA)
Mail: GPO Box 3 Melbourne VIC 3001
Phone: 1800 367 287
Fax: (03) 9613 6399
Email: info@afca.org.au
Website: afca.org.au

31.2 Please note however, that our EDR Scheme cannot deal with the matter unless there has first been an attempt to resolve it with us; and either:

(a) we have made a formal proposal to resolve the complaint, and we have been told that the proposal is not acceptable; or

(b) at least 45 days has elapsed since the complaint was made,

whichever event occurs sooner.

32. Limitation on the period of time after which we will not accept complaints

32.1 We will not accept a complaint from a User if we receive the complaint more than 6 years from the day that the User first became aware, or should reasonably have become aware, of the circumstances giving rise to the complaint.

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contact us

Police & Nurses Limited
ABN 69 087 651 876 AFSL 240701
Australian Credit Licence 240701

PO Box 8609
PERTH BC WA 6849
Tel: 13 25 77

pnbank.com.au

MS-087 (10/23)