

Terms and conditions

BOQ Specialist Online Service

Last updated: November 2023

Important Information

Except for BPAY® Payments, we only use the BSB and Account number to process payments and transfers to Accounts held with financial institutions other than BOQ Specialist. Please make sure the BSB and Account number you provide to us are correct. We will not verify the Account name you provide to us. If you believe you have made a mistake in an online transaction or payment, you must contact us as soon as possible on 1300 160 160. This line operates 24 hours a day and seven days a week. You must provide us with the full details so that we can locate the transaction and take action.

Products and services are provided by BOQ Specialist - a division of Bank of Queensland Limited ABN 32 009 656 740 AFSL and Australian credit licence No. 244616. By using such services, the User represents and warrants to BOQ Specialist that they have read, understood and agree to abide by such terms and conditions at all times. It is important that the User read these terms and conditions carefully and retain them for future reference. If the User does not understand or agree to abide by these terms and conditions, the User should not use the service.

The following terms and conditions apply to the provision of these services by BOQ Specialist:

- BOQ Specialist's Online Banking - **Part A**;
- The use of BPAY - **Part B**;
- Online Banking Services accessed via the BOQ Specialist Mobile App - **Part C1**; and
- Symantec Credential as set out in the 'Symantec Identity Protection End User Agreement' - **Part D**.

These terms and conditions should be read in conjunction with the terms and conditions of the Account which is accessed via Online Banking ("Other Terms"). Important information including information about features, and limits in respect of the Account is contained in the Other Terms. In the event of any inconsistency between provisions in different Parts, the provisions will apply in the following priority to the extent of any such inconsistency:

- Part C1; then
- Part A; then

- Part B and D; then
- Other Terms applicable to your Account

Part A

1. Definitions

Unless the context indicates otherwise, the following terms shall have the following meanings:

Account means any BOQ Specialist account (including any offset Account and credit card Account) with access to Online Banking.

Account Holder means the legal person who owns an Account and is responsible for the actions of all Users.

Authentication Code means a randomly generated six digit security code that BOQ Specialist may send to your mobile phone via SMS or Push Notification and is used to authenticate transactions and other activities that are deemed to require an additional level of security from time to time. In the event that the User does not have access to receive SMS or Push Notifications, the authentication code can be obtained by calling Client Service Centre.

Banking Business Day means a day that is not a Saturday, Sunday, banking holiday or public holiday in New South Wales, Australia.

Biller means an organisation which issues bills to customers, which customers can pay through the BPAY Scheme.

BOQ Specialist (we, us or our) means BOQ Specialist - a division of Bank of Queensland Limited ABN 32 009 656 740.

BOQ Specialist Mobile App means the computer application for use in connection with the Online Banking Services, which we make available for you to download and install on your mobile device from selected digital media stores.

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

BPAY Pty Ltd means BPAY Pty Ltd ABN 69 079 137 518.

BPAY Scheme means the BPAY electronic payments scheme through which a User may instruct us to make payments (BPAY payments) on your behalf to organisations (Billers) who are "Participating Billers" under the scheme. We will tell you if we cease to be a member of the BPAY Scheme.

BPAY View means an internet platform provided to BPAY Users through which you can receive or access bill summaries or access bill statements electronically from participating Billers nominated by you. BPAY and BPAY View are registered trademarks of BPAY Pty Ltd ABN 69 079 137 51.

Business EFT transaction means a transaction performed in the name of a User

that is not a Personal EFT transaction.

Card means a BOQ Specialist Credit Card and a BOQ Specialist Debit Card.

Cardlink Services Limited means Cardlink Services Limited ABN 60 003 311 644.

Client Number means the seven digit number given to the User by BOQ Specialist and is used to log onto Online Banking and the BOQ Specialist Mobile App. This number is also used to setup your access to the BOQ Specialist Mobile App on your phone.

Client Service Centre means the BOQ Specialist employee(s), agent(s), consultant(s) or subcontractor(s) who assist Users through the telephone numbers 1300 160 160 or 02 9293 2121 (or such other number as may be notified by BOQ Specialist from time to time).

Communication means communications between the User and BOQ Specialist exchanged by means of an e-communication, telephone and such other means of communication referred to in these terms and conditions or the Other Terms and used by BOQ Specialist from time to time, including other traditional means of communication.

Create Access means a type of Online Banking access for Delegated Users, which enables the Delegated User to create a Value Transaction, but not to authorise the Value Transaction. This means that the Value Transaction will not be processed by us until the appropriate Account Holder or Signatory authorises the transaction.

Credential ID means the static Symantec Credential number allocated to the User's Symantec Credential.

Delegated User is a person who is delegated the authority to act on behalf of an Account Holder. The Delegated User may be granted authority to act on all or a subset of the Accounts and limits to which the Account Holder has access. In addition, Account access can be restricted or the same as that to which the Account Holder has access.

Designated Account means the bank Account you have nominated to Us in writing in a form acceptable to Us (acting reasonably), as the Designated Account from which and to which payments to/from your Account are to be made.

Device has the meaning given to it in the ePayments Code.

e-communication means a message transmitted and received electronically in a manner and format that allows the message information to be presented to the recipient in a manner and format that is clear and readily understandable and allows the recipient of the message to retain the message information for subsequent reference, including communications to the User by means of the Website, the User's device, electronic terminal, computer, television or telephone or an electronic address nominated by the User.

ePayments Code means the ePayments Code administered by the Australian Securities & Investment Commission (previously the Electronic Funds Transfer Code of Conduct), as amended from time to time.

Execute Access means a type of Online Banking access for Delegated Users, which enables the Delegated User to perform (including to authorise) Value Transactions.

Instructions means an instruction from the User by means of a communication to perform a transaction or make a change to the Account setup.

Mistaken Internet Payment means a Personal EFT transaction which involves a payment by a User through a 'Pay Anyone' Online Banking service and processed by an ADI through direct entry where funds are paid into the Account of an unintended recipient because the User enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

- the User's error, or
- the User being advised of the wrong BSB number and/or identifier.

This does not include BPAY Payments.

Mobile App PIN means the four digit PIN used to protect access to the BOQ Specialist Mobile App installed on your Mobile Device. This is set when you first register the BOQ Specialist Mobile App on your Mobile Device.

Mobile Banking means the provision of Online Banking Services via the Website on the User's mobile phone or mobile device.

Mobile Device means a mobile telephone or other compact telecommunications device you use to perform Online Banking transactions or onto which you have installed the BOQ Specialist Mobile App.

Multi-to-sign means two or more authorised Signatories are required to operate the Account.

Online Banking means the provision of Online Banking Services provided to the User when they access the Website.

Online Banking Services means the internet banking services which we offer to you through the Website and the BOQ Specialist Mobile App which facilitate:

- (a) BOQ Specialist providing information about an Account to a User;
- (b) A User transmitting instructions to BOQ Specialist in relation to an Account; and
- (c) BOQ Specialist providing any other service in respect of online transactions to Users.

Online transactions means a banking transaction completed by accessing the Online Banking via the Website and the BOQ Specialist Mobile App using electronic equipment and forms part of the Online Banking Service.

Other Card Functions means credit card and debit card activations, PIN changes, placing or removing a temporary block on a Card and reporting a lost or stolen Card.

Other Terms has the meaning given to the term in clause 2.1.

Pass code has the meaning given in the ePayments Code.

Password means the secret password initially sent via SMS to the User's phone or provided verbally to the User, and which is changed by the User after the initial issuance and subsequently from time to time and is used by the User to log into Online Banking.

Pay Anyone is a facility available through Online Banking and the BOQ Specialist Mobile App that enables funds to be transferred from Accounts to Accounts held at most Australian financial institutions.

Payee means a third party bank Account established by the User for Online Banking and/or the BOQ Specialist Mobile App held at BOQ Specialist or any external Financial Institution.

Payment Cut-Off Time means the time set out in clause 8 of Part B.

Payment File Upload Facility means the service set out in clause 16.

Permissions means the types of access on one or more Online Banking Accounts granted by the Account Holder or Signatory to the Delegated User.

Personal EFT transaction means a transaction that is performed in the name of a User who is an individual for wholly or predominantly personal, domestic or household purposes.

Push Notification means an alert (typically a pop-up or other message) generated by the BOQ Specialist Mobile App when the App is not open, notifying the user of a new message which is sent to a registered mobile device.

Scheduled Payment means a request for a payment or transfer of funds for processing at a future date nominated by you.

Secure Message means a message sent via the secure messaging functionality provided within Online Banking or the BOQ Specialist Mobile App.

Security Code means the random number generated by the User's Symantec Credential, which is unique for every internet session.

Service means the BOQ Specialist banking, financial and related services accessed or used by the User by means of communications and includes the Online Banking service.

Signatory means an Account Holder or an authorised User (not a Delegated User) that acts on behalf of an Account Holder.

Symantec Credential means the credential provided in accordance with the multi factor authentication service known as the 'VIP Online Security Service' and associated with Symantec Inc, a Delaware Corporation. This credential may be provided to the User's mobile phone (soft credential) or provided in the form of a card (hard credential).

Transaction means a transaction in respect of the service including User set-up, making and managing payments, transfers and Account enquiries.

Unauthorised transactions has the meaning given to it in the ePayments Code.

User (or you) means the BOQ Specialist Account Holder authorised to use the service and to exchange communications and, where applicable, includes such person's duly authorised representative(s) such as Signatories on an account and Delegated Users.

Value transaction means an Online Transaction where an amount of funds is transferred from and/or to an Account.

Verification criteria means the minimum requirements that must be met by the User in order to verify the User's identity electronically, by telephone or otherwise, as reasonably determined by BOQ Specialist from time to time.

Verification mechanism means any mechanism, device or process used by BOQ Specialist to verify the identity of a User in the exchange of communications, including the Password, Security Code, Symantec Credential, Authentication Code and the online notification to the User when the User logs on to online transactions.

View Access means a type of Online Banking access for Delegated Users, which enables the Delegated User to view details of transactions and Accounts, such as Account balances.

Website means the BOQ Specialist website (including all its constituent web pages) on which BOQ Specialist provides the Online Banking Services from time to time located at www.boqspecialist.com.au.

Wording importing one gender shall include the other genders, words in the singular shall include the plural and vice versa and persons shall include natural persons and created entities.

2. Service and security

2.1 The Service shall, in addition to these terms and conditions, also be subject to the provisions of any other agreement concluded between the Account Holder and BOQ Specialist, including any Product Disclosure Statement and any other terms and conditions governing any BOQ Specialist products taken up by the Account Holder such as any product specific terms and conditions and any notices or communications given pursuant to those documents (collectively, "Other Terms"). In the event of any inconsistency between these terms and conditions and the Other Terms, these terms and conditions will prevail to the extent of the inconsistency for services provided, and transactions conducted, online.

2.2 The User shall, at the User's expense, be responsible for all steps necessary to acquire access to the online service (including obtaining equipment and services from an internet service provider and acquiring any device or medium which stores or receives the soft Symantec Credential) and for ensuring the security and confidentiality of any hardware, software, device, medium or Password or Mobile App PIN used by the User for such access.

2.3 If the User leaves the website via a link contained within the website and views content that is not provided by BOQ Specialist, the User does so at its own risk and acknowledges and agrees that BOQ Specialist is not responsible or liable for such content. The User acknowledges that no data transmission over the internet can be guaranteed to be totally secure and that there are inherent security risks with using e-communication and the online services and the User accepts those risks by using the service.

2.4 Subject to clause 18, BOQ Specialist does not make any representations, warranty or guarantee regarding the availability or operation of the service.

2.5 The Service may only be used on completion and acceptance of the requisite application forms, questionnaires, mandates and other documents provided or specified by BOQ Specialist from time to time, or as required under any applicable law.

2.6 BOQ Specialist shall not be bound in any manner until the documents described in clause 2.5 have been completed and/or submitted by the User and accepted by BOQ Specialist. BOQ Specialist reserves the right to reject, in its discretion, any application for the service.

2.7 The User acknowledges that BOQ Specialist will not be able to contact the User if BOQ Specialist does not have the User's updated personal information. The User agrees to advise BOQ Specialist of any change in the personal information the User has provided BOQ Specialist (including but not limited to the User's name, address and contact number(s)) as soon as is reasonably possible.

2.8 The User must notify BOQ Specialist immediately of any loss, theft or unauthorised use of a device or a breach of security by contacting the Client Service Centre on 1300 160 160.

3. Functionality provided by the Service

3.1 Our Online Banking Services includes the following:

- Transferring funds between linked/Designated bank Accounts;
- Making BPAY Payments;
- Payments to Accounts that are not linked to your Account (such as Accounts held with other financial institutions);
- Viewing monthly Account and tax statements and selecting statement preference (via online or hard copy paper statement);
- Obtaining Account information, such as Account balances;
- Offering a secure form of communication with us using Secure Messages;
- Providing Delegated User authority for another person to act on the Account Holder's behalf using Online Banking and assign the Permissions that person will have;

- Payments File Upload facility (schedule payments created using your own accounting software);
- Card management (including activating a Card, Card status changes and PIN reset);
- Updating personal details such as email, address and Tax File Number (TFN); and
- Providing maturity instructions for term deposit Accounts.

Not all banking services are available for all Accounts using Online Banking, Mobile Banking and the BOQ Specialist Mobile App. See the applicable product Other Terms for further information.

3.2 If an Account has a signing instruction where two or more Signatories are required to operate the Account, you may use Online Banking or the BOQ Specialist Mobile App to debit the Account via funds transfer or BPAY if at least two Signatories have authorised the transaction through Online Banking or the BOQ Specialist Mobile App. The Passwords, and Authentication Codes will be sent to the authorised Signatories, unless otherwise notified by us.

3.3 We may impose limits on your use of Online Banking and the BOQ Specialist Mobile App, including daily limits on withdrawals. **Details of the limits we impose in respect of an Account are set out in Clause 9 and in the Other Terms applicable to that Account. Other limits may apply as imposed by a merchant or other financial institution.**

3A. Users

3A.1 Types of Online Banking Users

3A.1.1 There are three types of people who can access Accounts through Online Banking:

- An Account Holder with authority to operate on the Account;
- A Signatory on an Account who has authority to operate on an Account and has been granted Online Banking access by the Account Holder and us; and
- Delegated User, who has been granted Online Banking access to the Account by an Account Holder or Signatory.

If you are an Account Holder, Signatory or Delegated User, your access to Online Banking will be through your unique Client Number and Online Banking Password.

3A.2 Delegated Users

An Account Holder or Signatory may delegate certain Online Banking access rights to a Delegated User. As the Account Holder, you will be responsible for the actions of all Delegated Users or Signatories accessing your Account through Online Banking.

The following rules apply to Delegated Users:

- The Account Holder or Signatory cannot grant a Delegated User greater

Online Banking access rights than the delegator's own access rights.

- Prior to Online Banking registration, a Delegated User will be required to submit an application form for Delegated User access that has been approved by an Account Holder or Signatory. Anti-money laundering (AML)/counter-terrorism financing (CTF) checks will be performed on the Delegated User.
- The Delegated User will be notified of their Client Number and temporary password.
- Once the Delegated User has received their credential they may register for Online Banking using online self-registration, or the assisted registration method through the Client Service Centre.
- The Delegated User may be able to transact on one or more of an Account Holders' Accounts after the Account Holder or Signatory has granted Permissions.
- The Account Holder or Signatory must choose the type of access that a Delegated User will have for each Account.
- The following types of access apply: View Access, Create Access and Execute Access.
- The Account Holder or Signatory may also choose not to grant a Delegated User access to a particular account or individual account function.
- The Account Holder or Signatory must set the daily limits for Accounts Transfer, Direct Debit, Pay Anyone Payments, BPAY Payments and Batch Payments made by the Delegated User, which may include lower (but not higher) limits than the Account Holder's or Signatories' own limits on their profile.
- Delegated Users cannot change the limits set for them.
- If you are a Delegated User, the Account Holder or Signatory may impose a limit on the transfer amount that you may perform on any one day.
- Multiple Delegated Users can be authorised to have access to Accounts.
- Any fees or charges incurred by the Delegated User accessing Online Banking are payable by the Account Holder.
- Delegated Users will not be able to activate a Card, change a PIN or change the Card status to blocked, lost or stolen.
- An Account Holder or Signatory may request that delegate access to their Account be permanently or temporarily disabled.
- Temporary disablement can be done through the Online Banking Delegated User functionality.
- An Account Holder or Signatory may request that delegate access to their Account be permanently or temporarily disabled.
- A Delegated User's access can be permanently disabled by contacting the Client Service Centre on 1300 160 160 or by sending a secure message through

Online Banking or through the BOQ Specialist Mobile App.

3A.2.1 Providing Permissions to a Delegated User

The Account Holder or Signatory must be logged on to Online Banking to provide Permissions to a Delegated User. If signing instructions on an Account are two or more to sign, then two Signatories will need to authorise the Permissions of the Delegated User. Once the Delegated User has been appropriately authorised, he or she can carry out transactions on Online Banking and via the Mobile App and other requests in accordance with the Permissions delegated.

3A.2.2 Managing a Delegated User's access

If an Account Holder or Signatory wishes to alter a Delegated User's access, the Account Holder or Signatory must do so through Online Banking. Account Holders or Signatories can monitor the activities of Delegated Users. They can nominate to receive an SMS, email or secure message alerts whenever the Delegated User carries out transactions. Account Holders or Signatories can also view full details of all activities carried out by Delegated Users.

Please note: Delegated User Permissions cannot be managed through the Mobile App.

4. Verification

4.1 BOQ Specialist may specify the verification mechanisms and verification criteria required to obtain access to the service from time to time.

4.2 The User must satisfy the verification criteria in respect of the service to obtain access.

4.3 BOQ Specialist shall be entitled to refuse to give effect to communications from a User and/or refuse a User's access to the service should a User fail to use the verification mechanism or fail to satisfy the verification criteria, as the case may be.

4.4 Only the User to whom the verification mechanism is allocated shall be entitled to use the service.

4.5 The User undertakes to enter the Security Code and change the Password on using the service for the first time and thereafter as required.

4.6 BOQ Specialist may require a User to enter an Authentication Code to authenticate a new Payee.

4.6.1 If you do not have a mobile number, have not provided your mobile number to us or are unable to receive an Authentication Code, you will need to contact the Client Service Centre to assist in the completion of the transaction.

4.6.2 Where an Authentication Code is required and is requested via SMS, the Transaction can only be completed if it is authenticated by using the Authentication Code. We will send the Authentication Code to your Australian mobile number. Following verification of the User, the client service consultant will provide the User with an Authentication Code to complete the transaction.

4.6.3 Where an approval via Push notification is required, the Transaction can only be completed if it is authenticated by approving the Push notification. We will send the Push notification to your registered mobile device.

4.7 BOQ Specialist may, acting reasonably, change the verification mechanism from time to time and the User undertakes to comply with the requirements of this new verification mechanism unconditionally. However, for personal EFT transactions, if the change has a material adverse impact on the User, BOQ Specialist will notify the User of the change and the User may, within 30 days after the date of such notification, terminate the Online Banking Services (without paying any early termination fees). If the User does not terminate the services within the 30 day period, the User will be deemed to have agreed to the change.

4.8 The User undertakes to ensure the confidentiality of the verification mechanism at all times, and shall without limitation, ensure that the verification mechanism is neither easily accessible nor disclosed to someone other than the User. For business EFT transactions, if storing or recording a Password on the User's computer, phone or network or misplacing, misusing or losing access to the Symantec Credential contributes toward any case of an unauthorised person performing an unauthorised transactions, you will be liable for all losses resulting from the Unauthorised transaction unless you have notified us of the relevant circumstances before the Unauthorised transaction occurred.

4.9 The User must not:

4.9.1 voluntarily disclose one or more of the Password, Mobile App PIN, Security Code or Authentication Code to anyone (including a family member or a friend);

4.9.2 indicate the Password on the outside of the Symantec device or keep a record of the Password (without making any reasonable attempt to protect the security of the Password) on one or on several articles carried with, or liable to loss or theft simultaneously with, the Symantec device;

4.9.3 select, as a Password or Mobile App PIN a numeric code which represents the User's birth date or an alphabetical code which is recognisable as part of the User's name and BOQ Specialist hereby specifically instructs the User not to do so and warns the User that if the User selects such a Password or Mobile App PIN, the User may be liable for losses arising from Unauthorised transactions caused by the User's selection of such a Password or Mobile App PIN. This is in addition to the warnings in the User guide provided to the User before the User is to select or change the password;

4.9.4 act with a degree of carelessness which greatly exceeds what would normally be considered careless behaviour (for example storing the User's Client Number and password for Online Banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "Online Banking codes"), in failing to protect the security of all Passwords, Mobile App PINs and Security Codes;

4.9.5 make the BOQ Specialist Mobile App installed on your Mobile Device, available to others; and

4.9.6 download, install or use the BOQ Specialist Mobile App on any device on which

the security features or standard User interfaces of the operating system have been bypassed or the underlying file system of the operating system has been accessed (included but not limited to instances of "jailbreaking", "rooting", "unlocking the bootloader" or using a debugging interface in respect of the device).

4.10 The User must enable and use the device lock for their Mobile Device (e.g. where a number or swipe pattern is required to be entered in order to unlock the Mobile Device for use).

4.11 The User must report the disclosure or possible disclosure of any of their Mobile App PINs, or the theft, loss, abuse, change or replication of your Mobile Device, as soon as you are aware of, or suspect, such an occurrence by telephoning the Customer Service Centre on 1300 160 160. You are responsible for any transactions on your Accounts up until the time we receive your report of such occurrence, and your failure to report any such occurrence may increase the Account Holder's potential liability for losses from Unauthorised transactions and losses to us arising from your breach.

4.12 We may take any appropriate measures in the interests of security, including but not limited to the actions set out in clause 4.13.1 to 4.13.4 below.

4.13 Where a User reasonably suspects that the verification mechanism has been or will soon be compromised, the User shall notify BOQ Specialist immediately by contacting the Client Service Centre. On receipt of the User's notification, BOQ Specialist reserves the right to:

4.13.1 reject all instructions received after the User's notification;

4.13.2 suspend the processing of all instructions not yet executed;

4.13.3 reverse (if possible) all executed transactions with effect from such date and time as BOQ Specialist may reasonably determine the unauthorised use to have commenced; and/or

4.13.4 deactivate access to the service without further notice to the User.

4.14 For business EFT transactions:

4.14.1 subject to clause 4.9, if a User provides any person with access to any verification mechanism or otherwise assists them to conduct or authorise a transaction in any manner whatsoever, such person shall be regarded as the User's duly authorised agent with full authority to use the service on the User's behalf; and

4.14.2 the User agrees that the verification mechanism used by BOQ Specialist will be sufficient confirmation of the User's identity unless BOQ Specialist either knows or ought reasonably know otherwise.

4.15 A Symantec Credential which is a hard token (card) will remain the property of BOQ Specialist, and BOQ Specialist reserves all rights in relation to the use of the card, including, but not limited to, the right to recall the card at any time. If BOQ Specialist recalls the card, BOQ Specialist will replace it with another equivalent security token/protocol to allow the User to authorise a Transaction

and otherwise access the Account.

5. Processing of instructions

5.1 The User can provide transfer instructions to BOQ Specialist in the following ways:

- i. by submitting a transaction in Online Banking or through the BOQ Specialist Mobile App;
- ii. by sending a Secure Message in Online Banking or through the BOQ Specialist Mobile App; or
- iii. by providing a signed instruction to Client Service Centre by email or fax.

For Multi-to-sign Accounts, a transfer instruction will only be submitted to BOQ Specialist for processing when a sufficient number of authorised Signatories have approved the transaction.

5.2 Except as described in clause 7.3 and Part B clause 5.2, the User's instruction contained in a communication becomes irrevocable once submitted to BOQ Specialist, and is an instruction to BOQ Specialist to effect the transaction in accordance with the provisions of these terms and conditions, the rules and procedures that apply to the service from time to time and in accordance with the instructions of the User.

5.3 The User shall not be entitled to issue a contrary command cancelling or reversing a previous command or amend any transaction once effected by BOQ Specialist.

5.4 Subject to clause 21.3, so long as the verification mechanism and verification criteria are satisfied:

5.4.1 BOQ Specialist shall not be obliged to verify the User's online transaction information; and

5.4.2 the User authorises BOQ Specialist to give effect to any communication which purports to emanate from the User, whether or not such communication was sent or authorised by the User. However, this will not affect your liability for Unauthorised transactions.

5.5 Acting reasonably, BOQ Specialist reserves the right to reject or suspend the execution of an instruction at any time should the value, frequency or destination of the instruction appear suspicious or out of the ordinary to BOQ Specialist. On so rejecting or suspending an instruction, BOQ Specialist undertakes to contact the User as soon as reasonably possible and to verify the instruction by such means as BOQ Specialist may reasonably determine.

5.6 The User undertakes to log off from Online Banking and the BOQ Specialist Mobile App in the prescribed manner and acknowledges that failure to log off could result in Unauthorised transactions which BOQ Specialist may not be liable for.

5A. Providing term deposit maturity instructions

5A.1 The User can provide term deposit maturity instructions to BOQ Specialist in the following ways:

- i. by contacting our Client Service Centre; or
- ii. in specific cases, by inputting maturity instructions into Online Banking or the BOQ Specialist mobile app.

Both methods are also subject to the Transaction and Savings Accounts Terms and Conditions available at www.boqspecialist.com.au/important-information/terms-and-conditions.

5A.2 Only AUD Term Deposits can accept an instruction via Online Banking. Foreign Currency term deposit maturity instructions will need to be provided to the Client Service Centre directly.

5A.3 The options available for reinvestment through Online Banking are:

- i. 30, 60, 90, 120, 180 day and 1 year terms only; and
- ii. Interest paid at maturity only.

To provide an instruction for a different term or interest payment schedule (i.e. interest paid monthly), please contact our Client Service Centre directly.

5A.4 Term deposit maturity instructions can be entered into Online Banking or the BOQ Specialist mobile app at any time from the start date of the term deposit up until 4pm the Business Day prior to the maturity date of the term deposit. Where a Term Deposit has more than one interest payment scheduled (e.g. interest paid monthly), maturity instructions can only be entered after the second last interest payment has been processed. If the User wishes to provide maturity instructions on or after the maturity date (subject to the 7-day grace period), they must contact our Client Service Centre directly.

5A.5 The User can change an existing maturity instruction via Online Banking or the BOQ Specialist mobile app at any time up until 4pm the Business Day prior to the maturity date. If the User wishes to provide changes to the maturity instructions on or after the maturity date (subject to the 7-day grace period), they must contact our Client Service Centre directly.

5A.6 If the instruction is to redeem all or part of the term deposit to an account that is not a Designated Account or an Account within the same BOQ Specialist entity, the User will need to contact our Client Service Centre who will facilitate this withdrawal.

5A.7 If you reinvest with the same amount or more or less funds, the interest rate applicable will be the prevailing interest rate on the date of maturity for the selected term and amount. This may be significantly different, higher or lower, to the interest rate applicable to your previous Term Deposit and the indicative rate displayed in Online Banking at the time you input your maturity instructions.

5A.8 Inputting a maturity instruction is subject to the signing instructions loaded against the account. For example: Any 1 to sign, 2 to sign etc.

6. Card management

6.1 Activation of a BOQ Specialist Card can be done using BOQ Specialist Online Banking and BOQ Specialist Mobile App.

6.2 The User can choose to temporarily block a Card to prevent unauthorised transactions if the Card has been misplaced by contacting our Client Service Centre on 1300 160 160 or by using the Temporary Block request in Online Banking and BOQ Specialist Mobile App.

6.3 If the Card has been lost or stolen, this can be replaced by contacting our Client Service Centre on 1300 160 160 or via Online Banking and BOQ Specialist Mobile App.

If the User has notified the Client Service Centre or via Online of the lost or stolen Card, the User still needs to contact our Client Service Centre to report any Unauthorised transactions on the Card.

6.4 An email notification will be sent to the User when a temporary block is applied to the Card or a lost or stolen Card has been reported via Online Banking or the BOQ Specialist Mobile App.

6A. Card activation and Card PIN management

6A.1 Activation of a Card or changing a PIN can be done via Online Banking or the BOQ Specialist Mobile App.

6A.2 The Card holder will receive a Push notification on the registered mobile device to activate the Card.

6B. Setting a temporary block on your Card

6B.1 By placing a temporary block on your Card, transactions will not be processed on the Card. However, the temporary block will not extend to any transactions via other additional Cards which are linked to your Accounts.

6B.2 If you place a temporary block on your Debit Card, transactions that are made only using the BSB and Account Number (as opposed to the Debit Card number) will still be processed.

6B.3 Once the selected Card is blocked, it cannot be used unless you unblock it. During this time, some of your regular payments may not be processed. You can unblock your Card via Online Banking or the BOQ Specialist Mobile App by contacting our Client Service Centre on 1300 160 160.

6B.4 We will be unable to decline or may otherwise still process transactions:

- that are not sent to us for authorisation e.g. transactions processed when there is a system interruption; and
- that are made without using the blocked Card.

6B.5 While we will make every effort to decline transactions while your Card is blocked, we cannot guarantee that all such transactions will be declined. We are

not responsible for any loss you suffer if a transaction is processed to your Card.

6B.6 The temporary block status is intended for temporary use only. The Bank may cancel or replace your Cards at any time after the temporary block has been set in accordance with the relevant Other Terms.

6B.7 A temporary block does not report your Card as lost or stolen. If your Card has been lost or stolen or you cannot locate your Card within 24 hours, you must report it as soon as possible via Online Banking or the BOQ Specialist Mobile App or by calling us. Should there be any fraudulent activity such as unauthorised transactions please contact us as soon as possible.

6C. Reporting lost or stolen Cards

6C.1 Reporting a Card lost or stolen will not block any transactions on any other Cards linked to your Account.

6C.2 If you report or mark your Debit Card as lost or stolen, transactions that are made only using the BSB and Account Number (as opposed to the Debit Card number) will still be processed.

6C.3 A replacement Card will automatically be issued when a Card has been reported lost or stolen via the Online Banking or the BOQ Specialist Mobile App. The replacement Card will be sent to the mailing address we hold on record. If you have recently moved, or have not updated your mailing address, or currently overseas, please contact our Client Service Centre on 1300 160 160.

7. Stopping or altering payments

7.1 Except for **BPAY**® Payments, we only use the BSB and Account number to process payments and transfers to Accounts held with financial institutions other than BOQ Specialist. Please make sure the BSB and Account number you provide to us are correct. We will not verify the Account name you provide to us.

7.2 If you believe you have made a mistake in an online transaction or payment, you must contact us as soon as possible on 1300 160 160. This line operates 24 hours a day, seven days a week. You must provide us with the full details so that we can locate the transaction and take action.

7.3 You may stop or alter an online transaction (including a **BPAY**® payment) that is a scheduled payment by amending the scheduled payment through Online Banking before midnight on the Banking Business Day immediately prior to the day the transaction or payment is to be made. Further information about stopping or altering **BPAY** payments is set out in Part B of these terms and conditions.

8. Transactions

8.1 The cut-off time for completed transactions entered directly by the User through Online Banking and the BOQ Specialist Mobile App is 4pm, Sydney time, on a Banking Business Day. Any transaction completed before 4pm on a Banking Business Day will be processed and value dated on the same Banking Business Day and will be deposited into the User's designated bank Account within 2 Banking Business Days after the transaction was completed. Any transaction completed after

4pm on a Banking Business Day or on a day that is not a Banking Business Day, will be processed and value dated on the next Banking Business Day and will be deposited into the User's designated bank Account within 3 Banking Business Days after the transaction was completed.

8.2 Online transfer requests received via Secure Message sent by the User must be received by 1pm (for Australian currency transactions) and 10am (for foreign currency transactions) Sydney time, Monday to Friday on a Banking Business Day. Secure Messages in relation to transactions received after 1pm (for Australian currency transactions) or 10am (for foreign currency transactions) on a Banking Business Day or on a day that is not a Banking Business Day, may be processed and value dated on the next Banking Business Day.

8.3 Future dated payments which fall on a non-Banking Business Day will be processed on the previous Banking Business Day. This applies to both 'once only' and scheduled payments.

8.4 Withdrawal transactions are limited to the User's available credit limits or cleared funds and paid to the User's nominated bank Account, or any Payee or Biller the User created for Online Banking and/or the BOQ Specialist Mobile App.

9. Transaction Limits

9.1 The following daily transaction limits apply by default in relation to Transactions performed using Online Banking Services by a Signatory, unless we have agreed or notified that a different transaction limit applies.

9.2 Daily transaction limits apply separately to each Signatory across all Accounts they are a Signatory to. Transactions performed by a Delegated User are also subject to any Account limits set by the Signatory.

Transaction Type	Daily Limits (per Signatory)
Pay Anyone payments	\$25,000
BPAY Payments	\$25,000
Designated Account payments	\$25,000
Total daily payments (including all Pay Anyone, BPAY Payments and Designated Account payments)	\$25,000
Own Accounts Transfer (transfers between Accounts by a Signatory to both the debited and credited Accounts)	Unlimited
Direct Debits	Unlimited

9.3 In our discretion, we may agree to increase the Pay Anyone payments, BPAY Payments, Designated Account payments or Total daily payments limits at your request. You can request that we increase any of these limits up to \$200,000 per day in Online Banking. Higher limits may be requested by contacting us. We will act

reasonably in considering any request to increase transaction limits.

9.4 You can request that any transaction limit be decreased in Online Banking or by contacting us.

9.5 We may also change any of the transaction limits that apply or impose new transaction limits without your agreement where we reasonably consider it appropriate or prudent to do so. If we do this, we will notify you as set out in clause 17.

9.6 Temporary increases may also be agreed to permit a Pay Anyone payment or Designated Account payment by contacting Us via phone, email or Online Banking secure message.

9.7 Merchants, or other financial institutions may also impose payment limits and restrictions.

10. Client Service Centre

10.1 Users may provide instructions via the Client Service Centre.

10.2 Users must satisfy the verification criteria, provided that even if a User has satisfied the verification criteria, a member of the Client Service Centre shall, acting reasonably, at all times have a discretion to refuse to give effect to an instruction where it is reasonably considered prudent to do so and, subject to clause 4, BOQ Specialist shall not be liable when a member of the Client Service Centre exercises such discretion on a reasonable basis. Reasonable reasons for such refusal may include, but are not limited to:

10.2.1 reasonable suspicion of attempted fraud;

10.2.2 reasonable suspicion of the User being forced against their will to perform a transaction;

10.2.3 BOQ Specialist reasonably having notified a member of the Client Service Centre not to execute instructions from a particular User or category of Users for whatever reason; or

10.2.4 A User being unreasonably abusive towards a member of the Client Service Centre.

10.3 Members of the Client Service Centre may require written confirmation or Secure Message from a User before giving effect to an instruction, in which event the instruction shall only be deemed to be received as provided for in clause 11.

10.4 The User grants BOQ Specialist the express authority to record telephone communications for future reference and acknowledges that such records may be used by BOQ Specialist for its own purposes including training, confirmation of instructions, seeking a resolution of disputes and may be submitted in evidence in any legal or administrative proceeding relating to the transaction.

11. Communications

11.1 You agree that we may give you any notices or other Communications or

documents we are required to give you in writing by publishing them or giving them to you in any manner allowed by law and any applicable code of practice. This may include giving you a notice or other document by:

11.1.1 Sending it to you by post to your last known residential or postal address;

11.1.2 If you have given us your email address, by sending it to you by email;

11.1.3 If you have given us your mobile number, by sending it to you by SMS;

11.1.4 Publishing it in a major national daily newspaper;

11.1.5 Placing it on or giving it to you with statements of Account;

11.1.6 Sending it to you by Secure Message in Online Banking; or

11.1.7 Publishing it on our Website or on our Online Banking sign-in page or within Online Banking and telling you we have done so (including by Secure Message).

11.2 An e-communication is deemed to have been sent - at the time shown on the e-communication as having been sent or, if not so shown, at the time shown on the sender's transmission logs as having been sent.

11.3 An e-communication from BOQ Specialist is deemed to be received by the User, when it is deemed to have been sent unless:

i. BOQ Specialist subsequently receives a delivery failure notice for the e-communication, or;

ii. clause 20.6 applies.

11.4 For the avoidance of doubt, the provisions of this clause 11 do not apply to the extent that they deem a device or Pass code to be received by the User on the basis that the device or Pass code has been sent to a User by mail or electronic communication to the User's correct mailing or electronic address.

12. Service charges

12.1 BOQ Specialist may charge the Account Holder for use of the service as set out in the Other Terms. In the event that BOQ Specialist does charge the Account Holder for the use of the service, the Account Holder shall authorise BOQ Specialist to debit a bank account nominated by the Account Holder with the charge in consideration for the use of the service.

12.2 BOQ Specialist shall, after giving the Account Holder reasonable notice of at least 30 days, be entitled to impose a charge or vary any charge from time to time subject to clause 12.1 and any applicable law or code which BOQ Specialist subscribes to.

12.3 Subject to clause 17.1, if any such variation in the charge is published on the website it shall be binding on the Account Holder from the date of such publication.

12.4 The Account Holder may be liable for government charges and taxes relating to transactions carried out in respect of the service.

13. Account balances

13.1 BOQ Specialist may provide transaction history and Account balance notification by mail, email, telephone and/or via the Online Banking Service from time to time on request from the Account Holder or Signatory.

13.2 BOQ Specialist does not warrant that Online Banking will be available at all times, will be uninterrupted or error-free.

13.3 BOQ Specialist will include any Account payment or transfer transactions performed through Online Banking on any Account statement provided to the Customer pursuant to the Other Terms that apply to the Account.

13.4 The Account Holder should check all entries in any transaction history or Account statement provided and any Account balance notification and promptly report to the Client Service Centre any apparent error or possible Unauthorised transaction.

14. Statement preferences

14.1 You can set your statement preference through Online Banking or through the BOQ Specialist Mobile App. There are two statement preference options available that can be selected:

- Receive an electronic version only.
- Receive both paper and an electronic version.

By electing to have Online Banking and/or Mobile Banking access, you agree and acknowledge that, with respect to your Account, all Account Holders, Signatories, and Authorised Delegates (with applicable permission) who have access to your Online Banking profile will be able to view your eStatements in Online Banking and/or the BOQ Specialist Mobile App.

14.2 If you activate eStatement preference, or the "Online" option, you acknowledge and agree that:

- eStatements will be made available in Online Banking and the BOQ Specialist Mobile App in accordance with the current statement cycle.
- When your Statement preference is set to "Online" only for your selected entity, notwithstanding any nomination or consent signed by you under National Credit Code (Code) for notices or other correspondence to be sent to a nominated person or address, you have agreed to receive eStatements in Online Banking and the BOQ Specialist Mobile App. All other notices and correspondence required to be sent by us under the Code will continue to be sent in accordance with any such nomination or consent (if applicable).
- If you are a non-individual entity (such as Company or Trust) Account Holder or Account Signatory any one Account Holder or Signatory can set the statement preference.

By activating Statement preference for the selected entity, you have agreed that

you are the signatory with authority to activate electronic statements on behalf of all signatories to the Accounts, you have obtained the consent of all signatories, and prior to obtaining that consent, and you have informed all signatories as the implications of their consenting to receive statements electronically.

15. Pop-up notices and browser settings

15.1 BOQ Specialist may publish notices to a User of Online Banking by way of "pop-up" windows or other means on the Online Banking website. The User must read all pop-up notices.

15.2 It is a condition of Online Banking that the User's internet service and browser permits pop-up notices from the BOQ Specialist Online Banking website to be displayed and pop-up notices shall be deemed to be read and accepted by the User.

16. Payments File Upload Facility

Payments file upload facility is available through Online Banking only.

If an Account Holder or Signatory grants a Delegated User access to batch payments, the Delegated User will also be able to perform Payment File Uploads. The Account Holder must have already registered to use Payments File Uploads before granting access to a Delegated User.

16.1 Features and benefits

This clause 16 only applies to business EFT transactions made through the Payments File Upload facility. Personal EFT transactions must not be made through the Payments File Upload facility.

Payments File Upload allows you to process bulk payments or direct debits by uploading a single debit or single credit data file which contains your instructions.

16.2 Authority to upload Payments File

To debit the accounts of third parties you need to be registered as a debit User of the Bulk Electronic Clearing System. In using this facility you must comply with the obligations of a debit User of the Bulk Electronic Clearing System as advised by us from time to time.

We will accept and distribute payments to most Australian financial institutions (separate files for each are not necessary). Please note that not all Australian financial institutions accept payments through the Bulk Electronic Clearing System.

To become a debit User of the Bulk Electronic Clearing System the Account Holder must complete a separate application. Completed and signed application forms may be submitted to our offices, or sent to us by mail or fax to;

Fax: (02) 9293 2160 Email: client.service@boqspecialist.com.au.

Within 10 days of approving your application we will send the Account Holder an Australian Payments Clearing Association number.

16.3 Setting up your access to Payments File Upload

To access Payments File Upload facility the Account Holder must have access to Online Banking.

All Online Banking Users with authority to make Batch Payments and/or Batch Debits on the relevant account will have access to the Payment File Upload facility.

16.4 **How to upload a debits data file**

Data files may be uploaded online by a User with access to Online Banking System.

The data file sent to us needs to be in the correct format. This format is called CEMTEX. You should be able to create a file in this format using an accounting package (such as MYOB). In addition, a file can be created manually on the Online Banking system even if a software package is not used.

A data file can be uploaded in the Online Banking system by selecting the 'Batch Debits' tab and clicking on 'Batch Debits Templates' option. Proceed to upload the file.

The data file must comply with the format and specifications described above. The data file sent to us must specify:

- the date on which the relevant debits are to be made into specified Accounts;
- details of the Accounts from which debits are to come from; and
- reference information that is to be displayed in the third party Account statement.

16.5 **Authorisation and payment**

By submitting the data file to us the Account Holder is authorising us to make the payments or debit the Accounts of third parties according to the instructions in the data file. Before forwarding the data file to us the User should check all the details in it carefully to ensure they are accurate. The User will also be given the opportunity to check these details once uploaded to the Online Banking system, but prior to confirmation of the data file, however the data file will not be able to be edited.

If instructions given in connection with this facility are incorrect, we will attempt to recover any incorrect payments on the Account Holder's behalf, but if we are unable to do so, we are not responsible for that payment.

Multi payment creation is not available through Mobile Banking. For Payment files, you must ensure cleared funds are available in the Nominated Account to meet the payment instructions, or have an approved processing limit which will allow us to debit the account(s) nominated. Provided that you comply with these terms and conditions and have sufficient funds available, we will accept and distribute payments to Accounts at participating financial institutions in accordance with your instructions.

If any payment or debit instructions to Accounts with other banks are dishonoured due to incorrect account details or insufficient funds in the case of debits, we may charge an administrative fee.

16.6 **Processing your instructions**

All payments in the data file will be made on the date nominated (provided that date is not in the past). If a past date is nominated we can, at our discretion, process the data file when we receive it or on the next Business Day if that date is a non-Banking Business Day. If a date in the future is nominated we will process the data file on that date or on the prior Banking Business Day if that date is a non-Banking Business Day.

Payments File Upload Transactions will be treated as received according to the cut-off times detailed in our Internet Banking Payments File Upload Facility application form.

If a data file is uploaded in error or there is an error in one or more payments within the file, we can stop the payment file from being processed if an instruction to cancel is received before 4.00pm on a Banking Business Day.

Payments File Upload Transactions are subject to the daily Online Banking Payments limit.

Debits File Upload Transactions are subject to the daily Online Banking Direct Debit limit approved by BOQ Specialist.

16.7 **Indemnity**

The Account Holder, severally indemnify each participating financial institution (including us) to which payment instructions are made using Payments File Upload. The Account Holder agrees to pay, the first time asked, any claim, action, demand, proceeding, loss, damage, expense or cost (including all legal costs and expenses) arising out of or resulting from:

- any payment made on the Account Holder's instructions or those of an authorised User which, at the time of that payment, were not authorised by the payer or to which the payee was not legally entitled;
- any payment made on the Account Holder's instructions or those of an authorised User which do not accord with the payer's request; or
- the failure to make a payment in accordance with the payer's request.

This indemnity may be enforced by any participating financial institution or by us as agent for any other participating financial institution. The Account Holder must pay the participating financial institution the amount of a demand made by that institution in accordance with this section 16.7 unless you are able to provide sufficient evidence that the payment was authorised by the relevant payer to the reasonable satisfaction of us of the participating financial institution. However, the Account Holder will not be taken to have admitted the validity of the demand by making a payment in accordance with it. On the Account Holder's request and at their expense, the participating financial institution concerned must provide the Account Holder with all reasonable assistance to investigate the circumstances on which that participating financial institution's demand was based.

If the Account Holder makes a payment to us or a participating financial institution

in response to a demand and is subsequently found to not be liable, the institution must refund to the Account Holder the amount of any demand paid by you to it.

16.8 Termination

The agreement for us to provide access to Direct Debit File Upload, the Account Holder, commences on the date we accept an application and continues until it is terminated in accordance with these terms and conditions. The Account Holder can terminate the agreement by giving us one weeks' written notice. If the Account Holder has not used the Payments File Upload services for more than 90 days, we can terminate the agreement by giving the Account Holder one weeks' written notice. Otherwise, we can terminate the agreement by giving you at least 30 days' written notice.

16A. Mistaken Internet Payments

16AA. If the User believes they have made or identified a Mistaken Internet Payment the User must immediately notify BOQ Specialist by calling the Client Service Centre on 1300 160 160.

16A.1 If a Mistaken Internet Payment is made and we are notified within 10 Banking Business Days of making the payment, then provided we are satisfied a Mistaken Internet Payment has occurred, we will contact the unintended payee's financial institution (the 'Other Financial Institution'). If:

- there are sufficient funds to the amount of the Mistaken Internet Payment ('Sufficient Funds') available in the Account of the unintended payee; and
- the Other Financial Institution is satisfied that a Mistaken Internet Payment has occurred,

the Other Financial Institution must return the funds to us within 5 to 10 Banking Business Days. We will then return the funds to the Account Holder as soon as practicable. If the Other Financial Institution is not satisfied that a Mistaken Internet Payment has occurred, the Other Financial Institution may seek the consent of the recipient account holder to return the funds.

16A.2 If a Mistaken Internet Payment is made and we are notified between 10 Banking Business Days and 7 months after making the payment, then provided we are satisfied a Mistaken Internet Payment has occurred, we will contact the Other Financial Institution, which will:

- investigate the matter within 10 Banking Business Days of our request to do so if there are Sufficient Funds available in the Account of the unintended payee;
- prevent the unintended payee from withdrawing the funds for a further 10 Banking Business Days if it is satisfied that a Mistaken Internet Payment has occurred; and
- return the funds to us within a further 2 Banking Business Days if the unintended payee does not establish they are entitled to the funds during the further 10 Banking Business Days period listed above.

We will then return the funds to the Account Holder as soon as practicable. If the Other Financial Institution is not satisfied that a Mistaken Internet Payment has occurred, the Other Financial Institution may seek the consent of the recipient Account Holder to return the funds.

16A.3 If a Mistaken Internet Payment is made and we are notified 7 months or more after making the payment, then provided we are satisfied a Mistaken Internet Payment has occurred, we will contact the Other Financial Institution. If:

- there are Sufficient Funds available in the Account of the unintended payee; and
- the Other Financial Institution is satisfied that a Mistaken Internet Payment has occurred,

the Other Financial Institution will seek the consent of the unintended payee to return the funds to us. If the unintended payee consents, the Other Financial Institution will return the funds to us. We will then return the funds to you as soon as practicable. If the Other Financial Institution is not satisfied that a Mistaken Internet Payment has occurred, the Other Financial Institution may seek the consent of the recipient Account Holder to return the funds.

16A.4 If the Account Holder is the recipient of a Mistaken Internet Payment, the Account Holder authorises us to withdraw the funds from the Account and return the funds to the payer's financial institution in accordance with our obligations under the ePayments Code.

16A.5 If BOQ Specialist and the Other Financial Institution are satisfied that a Mistaken Internet Payment has occurred, but there are not sufficient funds available in the unintended payee's Account, the Other Financial Institution must use reasonable endeavours to retrieve the funds.

16A.6 Where the unintended recipient of a Mistaken Internet Payment is receiving income support payments from Centrelink, the Other Financial Institution must recover the funds in accordance with the Code of Operation for Centrelink Direct Credit Payments.

16A.7 We will inform the Account Holder of the outcome of the reported Mistaken Internet Payment in writing within 30 Banking Business Days.

17. Amendments

17.1 BOQ Specialist may, in its sole discretion, subject to any legal requirements or the requirements of any code we subscribe to, vary these terms and conditions from time to time by giving the User advance notification of such variation by any means of communication (including through electronic communication if we have your consent to do so). We may send notices to you through various methods, including letter, Account statement, email, notification on the website or advertisement in the media.

17.2 For personal EFT transactions and periodic limits and other terms that relate to them, BOQ Specialist will provide at least 30 days prior written notification to the Account Holder (or such longer period as may be required by legislation or any code we subscribe to) if BOQ Specialist wishes to vary or modify these terms and

conditions to:

17.2.1 increase or impose a fee or charge (including a fee or charge relating to the issuing or replacing of a Passcode or device, or for performing a transaction);

17.2.2 increase the Account Holder's liability for losses relating to personal EFT transactions; or

17.2.3 impose, remove or change a daily or other periodic limit on transactions, a facility, or specific electronic equipment.

17.3 For any other changes to these terms and conditions or fees and charges, we will provide the User with notice of the change as soon as reasonably possible (which may be before or after the change is made) or, where the change is unfavourable, by providing the Account Holder with 30 days' notice.

17.4 Unless required by legislation or any code we subscribe to, no advance notice will be given if a change to these terms and conditions is required to immediately restore or maintain the security of a system or an individual facility, including the prevention of systemic or individual criminal activity, including fraud. BOQ Specialist can also give a shorter notice period (or no notice) of an unfavourable change if it is reasonable for us to manage a material and immediate risk.

17.5 The User agrees to implement and adhere to any reasonable procedures and/or restrictions imposed by BOQ Specialist from time to time in respect of the service. Subject to 17.4, BOQ Specialist rules, processes and procedures used in the operation of the service may be altered, replaced or withdrawn by BOQ Specialist in whole or in part in BOQ Specialist's full and absolute discretion, at any time.

18. Unavailability of Service

BOQ Specialist reserves the right, at any time, to alter, replace or discontinue the service in whole or in part, without notice to the User, if this is reasonably required to restore or maintain the security of the system or individual Accounts (including protecting the User from criminal activity such as fraud), in which event BOQ Specialist shall incur no liability whatsoever for the relevant damage (unless otherwise specified in clause 21).

19. Intellectual Property

Copyright in the Website and BOQ Specialist Mobile App and all materials made available through the Service is protected by both national and international intellectual property laws. Accordingly, any unauthorised copying, reproduction, communication, retransmission, distribution, dissemination, sale, publication, broadcast or other circulation or exploitation of any such material may constitute an infringement of that copyright. The trademarks, logos and service marks displayed on the Website and the BOQ Specialist Mobile App and materials made available through the service are registered and unregistered trademarks of BOQ Specialist.

Nothing contained in materials made available through the Service or on the

Website or the BOQ Specialist Mobile App should be construed as granting any licence or right to use any such trademarks, logos or service marks without the written permission of BOQ Specialist.

20. Transmission of Information

20.1 The User's attention is drawn to the fact that e-communications are susceptible to monitoring and interception.

20.2 The User is therefore discouraged from transmitting to BOQ Specialist any information which may be confidential, proprietary or sensitive by e-communications.

20.3 If a User sends an e-communication, BOQ Specialist will not be liable for any loss, harm or damage suffered by the User as a result of any compromise of the security of the User's devices or related electronic communication networks.

20.4 BOQ Specialist reserves the right to request independent verification of any information transmitted via email and the User consents to such verification from whatsoever source should BOQ Specialist reasonably deem it necessary.

20.5 Where the User has provided BOQ Specialist with relevant details to enable BOQ Specialist to communicate with the User by e-communications, the User agrees and consents to BOQ Specialist providing the User with any information that BOQ Specialist may be required to provide to the User by way of e-communication. The User must ensure that the e-communication details provided to BOQ Specialist are kept up-to-date and current.

20.6 The User agrees that any information BOQ Specialist is required to provide to the User (by writing or other means) may be provided by being made available at BOQ Specialist's electronic address (including on the website) for retrieval by e-communication to the User if:

20.6.1 BOQ Specialist promptly notifies the User by e-communication that the information is available for retrieval on the website and the nature of the information;

20.6.2 BOQ Specialist provides the User with the ability to readily retrieve the information by e-communication;

20.6.3 the User has viewed the information available at BOQ Specialist's electronic address (including on the website) and has been given the opportunity to retain that information for subsequent reference, including by saving or printing it, and the User specifically agrees that the User has viewed the information and has been given the opportunity to retain that information and that the User will not be otherwise provided with a copy of the information by BOQ Specialist (unless the User makes a separate request to BOQ Specialist for such information within 6 months of receipt of the e-communication); and

20.6.4 with respect to receipts for personal EFT transactions, the receipt is made available to the User at the same electronic address immediately on completion of the transaction in the manner and format as described in the definition of an "e-communication" in clause 1.

21. Liability and indemnity

21.1 The Account Holder is liable for losses resulting from unauthorised transactions:

21.1.1 where the User contributed to the losses through the User's fraud or the User's contravention of the requirements of clause 4.9, until such time when BOQ Specialist has been notified that a device has been misused, lost or stolen or that the security of any Passcodes has been breached;

21.1.2 where the User has contributed to losses resulting from unauthorised transactions by the User unreasonably delaying notification after becoming aware of the misuse, loss or theft of a device, or that the security of all Passcodes has been breached, where such losses occur between when the User became aware of the compromise (or should reasonably have become aware in the case of a lost or stolen device) and when BOQ Specialist was actually notified; or

21.1.3 for business EFT transactions, as otherwise provided by these Online Banking terms and conditions or by any Other Terms in which these Online Banking terms and conditions are incorporated.

For personal EFT transactions, the Account Holder's liability under this clause 21.1.3 is limited to, in the case of 21.1.1 and 21.1.2, the applicable daily or periodic transaction limit(s) or the balance on the Account (including any prearranged credit) from which the losses were incurred and, if a Passcode is required to perform the transaction, and clause 21.1.1 and 21.1.2 do not apply the Account Holder is liable for the least of:

- (a) \$150; or
- (b) the balance of those Accounts (including any pre-arranged credit) from which value was transferred in the unauthorised transactions and which BOQ Specialist and the Account Holder has agreed may be accessed using Online Banking;
- (c) or the actual loss at the time BOQ Specialist is notified that the device has been misused, lost or stolen or that the security of the Passcodes has been breached (excluding that portion of the losses incurred on any one day which exceed any applicable daily transaction or other periodic transaction limit(s)).

For personal EFT transactions, in the case of 21.1.1 and 21.1.2, the Account Holder will not be liable for losses incurred on any Accounts which the User and BOQ Specialist had not agreed could be accessed using Online Banking or the BOQ Specialist Mobile App.

For losses covered by clause 21.1.1, if more than one Passcode is required to perform a transaction and BOQ Specialist proves that a User breached the security requirements in 4.9 for one or more of the Passcodes, but not necessarily all of them, the Account Holder is liable where BOQ Specialist can prove that on the balance of probability the breach of the Passcode was more than 50% responsible for the loss.

For personal EFT transactions, in considering whether a User contributed to the loss under 21.1.1 and 21.1.2 we will ensure that we consider all reasonable evidence, including whether the User left their card in an ATM, and whether the ATM

incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM. The fact that a facility was accessed using a device and/or Passcode is not in itself determinative and the use or security of any information required to perform a transaction that is not required to be kept secret is not relevant to an Account Holder's liability.

21.2 Subject to clause 21.1.3, for personal EFT transactions, BOQ Specialist accepts that the Account Holder is not liable for losses:

21.2.1 that are caused by the fraudulent or negligent conduct of employees or agents of BOQ Specialist or companies involved in networking arrangements or of merchants or of their agents or employees;

21.2.2 relating to any device, identifier or Passcode which is forged, faulty, expired or cancelled;

21.2.3 that arise from transactions which require the use of a Password, Mobile App PIN, device, Authentication Code that occurred before the User received any such Password, Mobile App PIN, device, Authentication Code (including a reissued device and/ or Passcode). If there is a dispute about whether a Passcode was received, it is presumed that a User has not received the Passcode unless we prove otherwise;

21.2.4 that are caused by the same transaction being incorrectly debited more than once from the same Account;

21.2.5 resulting from unauthorised transactions:

(a) occurring after the User has notified BOQ Specialist's Client Service Centre that a device has been misused, lost or stolen or that the security of a Passcode has been breached; or

(b) where it is clear that the User has not contributed to such losses;

21.2.6 caused by the failure of BOQ Specialist's system or equipment to complete a transaction accepted by BOQ Specialist's system or equipment in accordance with the User's instructions and BOQ Specialist does not deny, implicitly or explicitly, a right to the Account Holder to make claims for consequential damage which may arise as a result of a malfunction of BOQ Specialist 's system or equipment however caused, except where the User should have been aware that the system or equipment was unavailable for use or was malfunctioning, in which case BOQ Specialist limits its responsibilities to the correction of any errors in the account, and the refund of any charges or fees imposed on the Account Holder as a result.

21.3 For business EFT transactions, the Account Holder agrees to indemnify BOQ Specialist, its officers and employees, ("Indemnified Persons") and hold such Indemnified Persons harmless against any loss, damage, taxes, cost, expense (including reasonable legal fees), claim, proceeding or liability of any kind (other than that arising from the negligence, mistake, wilful misconduct or fraud by such Indemnified Persons) which the Indemnified Persons may suffer or incur as a result of the User's breach of these terms and conditions or the use of the service or the website.

21.4 BOQ Specialist is liable for any loss that occurs while its process for reporting

unauthorised transactions, loss, theft or misuse of a device or a breach of security of a Passcode is unavailable, provided that a report is made within a reasonable time of the process again becoming generally available (unless the unavailability is the User's responsibility).

21.5 For the avoidance of doubt, liability for losses resulting from unauthorised personal EFT transactions will be determined in accordance with the ePayments Code.

21.6 Subject to clause 4.9, once a User has advised us that their Mobile App PIN has been disclosed and/or a Mobile Device has been lost or stolen, and except if a User has acted fraudulently or negligently, the Account Holder will not be responsible for any unauthorised use of them after that time.

The Account Holder will be liable to pay no more than \$50 of any loss that occurs before we are notified.

However, this \$50 limit will not apply if:

- (a) the User acted fraudulently or negligently; or
- (b) the User breached the Terms and Conditions in a manner that caused the loss; or the User directly contributed to the unauthorised use of the Online Banking Services by, for example (but not limited to), selecting a Mobile App PIN contrary to cl. 4.9.3, failing to reasonably safeguard a Mobile Device, keeping a written record of a Mobile App PIN without taking reasonable steps to ensure its security, parting with their Mobile Device, or disclosing a BOQ Specialist Mobile App PIN to any other person (other than as allowed under the Terms and Conditions), failing to take all reasonable steps to prevent disclosure to any person when keying in a Mobile App PIN, or unreasonably delaying notification to us of the loss or theft of the Mobile Device, or of the actual or possible disclosure to any other person of a Mobile App PIN.

If any of these apply, the Account Holder's maximum liability will be the lesser of:

- (a) the actual loss at the time of notification; or
- (b) the maximum amount that would have been entitled to be withdrawn from the Account between the time the Mobile Device was lost/stolen and the time we are notified; or
- (c) if the ePayments Code applies, the maximum liability permitted by the ePayments Code.

22. Assistance by the Client Service Centre regarding verification mechanism

22.1 In the event that the User forgets or misplaces their Online Banking Password, BOQ Specialist will provide the User with such information, via SMS, or over the phone by a member of the Client Service Centre, subject to clauses 22.2 and 22.3 below and any other reasonable conditions BOQ Specialist may impose ("the disclosure").

22.2 BOQ Specialist shall determine the verification criteria for the member of the Client Service Centre to verify the User for purposes of the disclosure but such criteria will be reasonable.

22.3 After the member of the Client Service Centre has provided the User with a temporary Password, the User must immediately access the website and change the Password. For business EFT transactions, the Account Holder shall be held liable for any loss, claim, damage, expense or tax which the Account Holder may suffer or incur as a direct result of the failure to change the password in accordance with this clause.

22.4 Members of the Client Service Centre are bound by the confidentiality provisions contained in these terms and conditions.

23. Jurisdictional disclaimer

Unless otherwise agreed with BOQ Specialist, the service is only available to:

23.1 persons domiciled or of permanent residence in Australia;

23.2 corporate or other legal entities or organisations domiciled and incorporated in terms of the laws of Australia; and

23.3 Australian citizens resident outside Australia, provided such residents Appoint an Australian agent and use funds held in an Australian bank Account.

24. General

24.1 The User acknowledges and accepts that BOQ Specialist shall be entitled in its sole and absolute discretion to monitor, intercept, record and use as evidence all instructions between the User and BOQ Specialist at any time including the use of Online Banking and the BOQ Specialist Mobile App.

24.2 Use of the service shall not in any way vary any aspect of the banker/client relationship between the Account Holder and BOQ Specialist. In particular the Account Holder acknowledges that:

24.2.1 the use of the service shall not entitle the Account Holder to overdraw on any Account, unless prior Approval has been granted by BOQ Specialist; and

24.2.2 the credit limits (if any) allocated to the Accounts shall not be exceeded.

24.3 In effecting any transaction BOQ Specialist shall not act nor shall it be deemed to be acting as the Account Holder's agent nor as the agent of any payee.

24.4 The Account Holder shall not cede, assign, make over or transfer to any other person, firm or company any of the Account Holder's rights or obligations in respect of, or arising out of, these terms and conditions or the use of the service without BOQ Specialist's prior written consent. BOQ Specialist may cede, assign, make over or transfer any of its rights or both its rights and obligations under these terms and conditions and/or in respect of the service to any person, firm or company without notice to the Account Holder, provided that, where the Account Holder acquired the services wholly or predominantly for personal, domestic or household use or consumption, the person to whom BOQ Specialist novates or transfers its

obligations under these terms and conditions must have the ability to meet the obligations novated or transferred to it.

24.5 The User warrants that they will comply with all applicable laws when using the service.

24.6 The User consents that any disputes arising in connection with the service, or these terms and conditions or any matter related to or in connection therewith is governed by and construed in accordance with the law for the time being in force in New South Wales, Australia, and each party agrees to submit to the non-exclusive jurisdiction of the courts of that place.

24.7 We warrant that we comply with the ePayments Code in relation to personal EFT transactions.

24.8 As part of our commitment to customer service, we have adopted the Banking Code of Practice (**BCOP**). This is a self-regulatory code which aims to foster good relations between banks and customers, and to promote good banking practice. The BCOP applies to banking services provided to customers who are "individuals" or "small businesses" as defined in it. We will comply with the BCOP, where it applies to the banking services we provide.

The BCOP requires us to provide you with certain information. You will find this information in this document (and, where applicable, the Other Terms), and on request.

25. Access to personal information

25.1 The User grants BOQ Specialist (including its agents and contractors) authority to monitor, keep record of and have access to all forms of correspondence or communications in relation to the User received by or sent from BOQ Specialist or any of its employees, agents or contractors.

25.2 If BOQ Specialist accepts a suretyship/s or other security from a third party, the Account Holder acknowledges and agrees that BOQ Specialist may provide the surety or other third party with information about the Account Holder, including the Account Holder's confidential financial information.

25A. Updating personal details

25A.1 Personal details can be updated in Online Banking, the BOQ Specialist Mobile App or by contacting our Client Service Centre on 1300 160 160.

25A.2 The following personal details can be updated via Online Banking or the BOQ Specialist Mobile App:

- Email address;
- Mobile number;
- Residential address;
- Mailing address;

- Provide Tax File Number (TFN)

25A.3 We will process changes to personal details updated via Online Banking or the BOQ Specialist Mobile App as soon as reasonably possible.

26. Disputes and complaints

If you have a problem, complaint or dispute

26.1 Our service commitment

At BOQ Specialist we are committed to providing our customers with innovative banking solutions and the best customer service experience. Resolution of problems is a priority for us. If at any time our service does not meet your expectations we would like you to let us know.

(a) How to contact us

If you have a complaint, there are a number of ways to contact us:

- Contact your local branch manager or Business Banker
- Call us on 1300 160 160, 24 hours a day, 7 days a week
- Complete the online complaints form at www.boqspecialist.com.au/feedback-and-complaints
- Contact our Customer Relations Department via:

Email: customer.relations@boqspecialist.com.au

Call: 1800 663 080

Write to: Customer Relations Reply Paid 2258 Brisbane QLD 4001

(b) How will your complaint be handled?

If we cannot solve your problem on the spot, we will let you know who is handling your complaint and how long it is likely to take for it to be resolved. For further information about how we handle complaints, ask our friendly staff for a copy of our Complaint Guide or alternatively download a copy available on our website.

(c) What to do if you feel your complaint has not been resolved

If you're unhappy with our response you can approach the Australian Financial Complaints Authority (AFCA). AFCA provides a free and independent complaint resolution service for financial services. To contact them you can:

Call: 1800 931 678

Email: info@afca.org.au

Online: www.afca.org.au

Write to: GPO Box 3 Melbourne VIC 3001

The Australian Securities and Investments Commission (ASIC) has an information line: 1300 300 630. You can use this number to make a complaint and obtain further

information about your rights.

27. Privacy and Information Collection

BOQ Specialist collects and handles personal information as described in the Account Application Form, Other Terms and the BOQ Specialist Privacy Policy, and as otherwise notified to or agreed by the User. The BOQ Specialist Privacy Policy is available at boqspecialist.com.au or by contacting us on 1300 160 160.

28. Confidentiality

We have a duty of confidentiality towards the User except in circumstances where:

- (a) disclosure is compelled by law;
- (b) there is a duty to the public to disclose;
- (c) the interests of BOQ Specialist require disclosure; or
- (d) disclosure is made with your express or implied consent.

29. Termination and suspension

The agreement for us to provide Online Banking and the BOQ Specialist Mobile App to you, the Account Holder, commences on the date we accept your application and continues until it is terminated in accordance with these terms and conditions.

29.1 When we can terminate your access to Online Banking and the BOQ Specialist Mobile App

We can cancel your access to Online Banking and the BOQ Specialist Mobile App without reason by giving you reasonable prior notice of not less than 30 days.

We may also cancel an Online Banking Service, at any time, without giving you prior notice, if:

- we are required to do so by law or in order to comply with our legal or other regulatory obligations (including Card scheme and payment system rules);
- you don't provide us with information we reasonably require to verify your identity or the source of any funds deposited into the Account or to otherwise comply with our legal obligations or other regulatory obligations (including Card scheme and payment system rules);
- you don't provide us with accurate and up to date Foreign Tax Residency Status information; or
- we reasonably believe that:
 - doing so is necessary to prevent loss to you or us;
 - the Account or Online Banking Service is being used in a manner that may result in loss to you or us;
 - there is fraudulent activity occurring in relation to your Account or Online Banking Service;

- the Account or Online Banking Service is being operated in breach of these terms and conditions in a way that increases risk to you or us;
- your use of the Account or Online Banking Service or activities you undertake in connection with the Account or Online Banking Service are at high risk of involving fraudulent or other unlawful behaviour or loss to us or other persons (for example, activities that are at high risk of being involved in scams);
- you or the Account holder provided us with false or misleading information when we opened the Account or issued the Online Banking Service which materially increases the risks we are exposed to in relation to you or the Account or Online Banking Service and we would not have opened the Account or issued the Online Banking Service had the correct information been provided to us; or
- the Account or Online Banking Service is being used to defame, harass or threaten any person, or to promote or encourage physical or mental harm of any person or to promote violence against any person (including in the use of the payment descriptions and/or references).

29.2 When you can terminate your access to Online Banking and the BOQ Specialist Mobile App Account Holders can cancel all Online Banking and the BOQ Specialist Mobile App access to their Accounts by contacting the Client Service Centre via phone or Secure Message. Account Holders can request that access to Online Banking and the BOQ Specialist Mobile App be reinstated.

For cancellation of access in relation to Users other than the Account Holder, see section 3A.2. Delegated Users can also request that we cancel their Online Banking and the BOQ Specialist Mobile App access. Requests should be made via Secure Message. Online Banking and the BOQ Specialist Mobile App access for Delegated Users may be reinstated upon request from the Account Holder by contacting the Client Service Centre.

Online Banking for Delegated Users must be reinstated by the Account Holder.

29.3 When we can suspend your access to Online Banking and the BOQ Specialist Mobile App

We may suspend an Online Banking Service, at any time, without giving you prior notice, if:

- we are required to do so by law or in order to comply with our legal or other regulatory obligations (including Card scheme and payment system rules);
- you don't provide us with information we reasonably require to verify your identity or the source of any funds deposited into the Account or to otherwise comply with our legal obligations or other regulatory obligations (including Card scheme and payment system rules);
- you don't provide us with accurate and up to date Foreign Tax Residency Status information; or

- we reasonably believe that:
 - doing so is necessary to prevent loss to you or us;
 - the Account or Online Banking Service is being used in a manner that may result in loss to you or us;
 - there is fraudulent activity occurring in relation to the Account or Online Banking Service;
 - the Account or Online Banking Service is being operated in breach of these terms and conditions in a way that increases risk to you or us;
 - your use of the Account or Online Banking Service or activities you undertake in connection with the Account or Online Banking Service are at high risk of involving fraudulent or other unlawful behaviour or loss to us or other persons (for example, activities that are at high risk of being involved in scams);
 - you or the Account holder provided us with false or misleading information when we opened the Account or issued the Online Banking Service which materially increases the risks we are exposed to in relation to you or the Account or Online Banking Service and we would not have opened the Account or issued the Online Banking Service had the correct information been provided to us; or
 - the Account or Online Banking Service is being used to defame, harass or threaten any person, or to promote or encourage physical or mental harm of any person or to promote violence against any person (including in the use of the payment descriptions and/or references).

We will act reasonably when suspending an Online Banking Service and we will not do more than is reasonably necessary considering the reasons why we have taken such action. We will tell you if we suspend your Online Banking Service and, where possible, we will tell you what you need to do for us to reinstate it.

Part B

1. **BPAY** terms and conditions

1.1 The **BPAY** terms and conditions set out in this Part B apply if we are asked to make a payment on an Account Holder's behalf through the **BPAY** Scheme. These terms and conditions apply in addition to the terms in Part A. We are a member of the **BPAY** Scheme. We will tell the Account Holder if we are no longer a member of the **BPAY** Scheme.

1.2 You may choose to make a **BPAY** Payment using Online Banking or the BOQ Specialist Mobile App.

1.3 When you ask us to make a **BPAY** Payment, you must give us the information specified in clause 4 below. We will then debit the Account you specify with the amount of that **BPAY** Payment. We may decide not to make a **BPAY** Payment if there

are insufficient cleared funds in the Account at the time when you tell us to make that payment.

1.4 When we make a **BPAY** Payment we are not acting as your agent or the agent of the Biller to whom that payment is directed.

2. How to use **BPAY**

2.1 You can ask us to make **BPAY** Payments from an Account if these terms and conditions and the Other Terms permit you to make withdrawals by **BPAY** Payments from that Account.

2.2 A **BPAY** Biller may set limits on the amount of a **BPAY** Payment to that Biller. Some Billers will not accept **BPAY** Payments from certain Accounts (for example, credit card Accounts).

2.3 If there is any inconsistency between these terms and conditions and the **BPAY** Scheme terms and conditions set out in this Part B, then the **BPAY** Scheme terms and conditions will apply to the extent of that inconsistency.

2.4 If we allow a credit card to be used to pay a bill through the **BPAY** Scheme, we will treat that payment as a credit card purchase transaction.

2.5 A mistaken or erroneous payment received by a Biller from another person does not constitute under any circumstances part or whole satisfaction of any underlying debt owed between you and that Biller.

3. Valid payment direction

We will treat any instruction to make a **BPAY** Payment as authorised by the Account Holder if, when it is given to us your Customer Number, Password and Symantec Security Code are entered and the **BPAY** Payment is made through Online Banking or BOQ Specialist Mobile App.

4. Information you must give us

4.1 To instruct us to make a **BPAY** Payment, we must be given the following information:

- (a) the Account from which we are to debit the payment;
- (b) the amount to pay;
- (c) the biller code of the Biller to pay (this can be found on the bill); and
- (d) your customer reference number (this can be found on Accounts or invoices you receive from Billers).

4.2 We are not obliged to effect a **BPAY** Payment if you do not give us all the above information or if any of the information you give us is inaccurate.

5. Stopping or altering payments

5.1 If you believe that you have made a mistake in a **BPAY** Payment, you must contact us as soon as possible on 1300 160 160 24 hours a day, seven days a week

and give full details so that we can locate the transaction and take action.

5.2 You may stop or alter a **BPAY** Payment that is a Scheduled Payment by amending the request through Online Banking before midnight on the Banking Business Day immediately prior to the day the transaction or payment is to be made.

5.3 We cannot accept a request to stop or alter a **BPAY** Payment that is not a Scheduled Payment after you have instructed us to make it.

5.4 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, if you tell us to make the **BPAY** Payment before our Payment Cut-Off Time (see clause 8) on a Banking Business Day; or

(b) on the next Banking Business Day, if you tell us to make a **BPAY** Payment either after our Payment Cut-Off Time (see clause 8) on a Banking Business Day or on a non-Banking Business Day.

5.5 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 our 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.

5.6 While it is expected that any delay in processing a **BPAY** Payment for any reason set out in clause 5.5 will not continue for more than one Banking Business Day, any such delay may continue for a longer period.

5.7 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. Liability for **BPAY mistaken payments, unauthorised transactions and fraud**

6.1 **BPAY** participants undertake to promptly process **BPAY** Payments. You must tell us promptly:

(a) if you become aware of any delays or mistakes in processing the **BPAY** Payments;

(b) if you did not authorise a **BPAY** Payment that has been made from an Account; or

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

6.2 We will attempt to rectify any such matters in relation to your BPAY Payments in the way described in clauses 6.3 to 6.5.

If the ePayments Code applies to an Account and a BPAY Payment is made on the Account without your knowledge or consent, liability for that unauthorised BPAY Payment will be determined in accordance with clause 21 of Part A of the Online Banking Terms and Conditions. Otherwise, except as set out in clauses 6.3 to 6.5 and clause 11, we will not be liable for any loss or damage you suffer as a result of using the BPAY Scheme where we and our employees, agents or appointed-receivers have not been negligent, fraudulent or guilty of wilful misconduct.

6.3 If a BPAY Payment is made to a person or for an amount which is not in accordance with your instructions (if any), and an Account was debited for the amount of that payment, we will credit that amount to the 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.

6.4 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 the Account with the amount of that unauthorised payment. However, the Account Holder must pay us the amount of that unauthorised payment if:

(a) we cannot recover that amount within 20 Banking Business Days of us attempting to do so 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.

6.5 If a BPAY Payment is induced by the fraud of a person involved in the BPAY Scheme, then that person should refund the Account Holder the amount of the fraud-induced payment. However, if that person does not refund the Account Holder the amount of the fraud induced payment, the Account Holder 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 we will attempt to obtain a refund for the Account Holder of the fraud induced payment.

6.6 If a BPAY Payment falls within the type described in clause 6.4 and also clause 6.3 or 6.5, then we will apply the principles stated in clause 6.4.

6.7 If a BPAY Payment falls within both the types described in clauses 6.3 and 6.5, then we will apply the principles stated in clause 6.5.

6.8 Except where a BPAY Payment is a mistaken payment referred to in clause 6.3, an unauthorised payment referred to in clause 6.4, or a fraudulent payment referred to in clause 6.5, BPAY Payments are irrevocable. No refunds will be provided through the BPAY Scheme where the Account Holder has a dispute with the Biller about any goods or services. Any dispute must be resolved with the Biller.

6.9 The Account Holder's obligation under clauses 6.3 and 6.4 to pay us the amount of any mistaken or unauthorised payment (as applicable) is subject to any of the Account Holder's rights referred to in clause 11.

6.10 The Account Holder indemnifies 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 the User:

- (a) did not observe any of your obligations under this Part B; or
- (b) acted negligently or fraudulently in connection with these terms and conditions.

However, the Account Holder is not liable for any loss or damage to the extent caused by the fraud, negligence, mistake or wilful misconduct of us or our employees, agents or appointed receivers.

6.11 If we are told that a BPAY Payment made from an Account is unauthorised, the Account Holder must first give us written consent addressed to the Biller who received that BPAY Payment, consenting to us obtaining from the Biller information about the Account with that Biller, 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. If you do not give us that consent, the Biller may not be permitted under law to disclose to us information we need to investigate or rectify that BPAY Payment.

7. Suspension

We may suspend your right to participate in the BPAY Scheme at any time if you or someone acting on your behalf is reasonably suspected by us of being fraudulent.

8. Cut-off times

If you tell us to make a BPAY Payment before the times specified, it will in most cases be treated as having been made on the same day. Payment Cut-off times (for BPAY Payments): 7 days a week, 4.00pm. However, if you tell us to make a BPAY Payment on a Saturday, Sunday or a public holiday or if another participant in the BPAY Scheme does not process a BPAY Payment as soon as they receive its details, the payment may take longer to be credited to a Biller.

9. When a Biller cannot process your payment

If we are informed that your payment cannot be processed by a Biller, we will:

- (a) inform you of this;
- (b) credit your Account with the amount of the BPAY Payment if it has been taken out of your Account; and
- (c) if you ask us to do so, take all reasonable steps to assist you in making a BPAY Payment to that Biller as quickly as possible.

10. Account records

You should check your Account records carefully and promptly report to us as soon as

you become aware of 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.

11. Consequential damage

11.1 This clause does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed. If those laws or that code would make this clause illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this clause is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.

11.2 We are not liable for any consequential loss or damage the Account Holder suffers as a result of using the BPAY Scheme, other than due to any loss or damage suffered due to our or our employees or agent's, negligence, wilful misconduct or fraud or that of any receiver we have appointed 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.

12. Privacy

12.1 The Account Holder agrees to our disclosing to Billers nominated and if necessary the entity operating the BPAY Scheme (BPAY Pty Ltd) and any agent Appointed by it from time to time, including Cardlink Services Limited, that provides the electronic systems needed to implement the BPAY Scheme:

(a) such of their personal information (for example name, email address and that the Account Holder is our customer) as is necessary to facilitate your registration for or use of the BPAY Scheme;

(b) such of the Account Holder's transactional information as is necessary to process, rectify or trace BPAY Payments.

(c) The Account Holder's BPAY Payments information will be disclosed by BPAY Pty Ltd, through its agent, to the Biller's financial institution and information necessary to process the use of BPAY View will be disclosed by BPAY Pty Ltd, through its agent, to the Biller. Also, we may disclose such of the Account Holder's transactional information as is necessary to rectify or trace a BPAY Payment made by mistake to the Biller that received the payment and the Biller to whom the Account Holder intended to make the payment or the financial institution of either or both Billers.

12.2 You must notify us, if any of the personal information we hold about you changes and you consent to us disclosing your updated personal information to all other participants in the BPAY Scheme referred to in this clause as necessary.

12.3 You can request access to your information held by us by contacting us, or held by BPAY Pty Ltd by contacting BPAY Pty Ltd or its agent, Cardlink Services Limited.

Part C1

Before using the BOQ Specialist Mobile App to access Online Banking Services please read the following Terms and Conditions

1. You can use the BOQ Specialist Mobile App to access a range of Online Banking Services, including:
 - (a) view Accounts of all entities that you are an Account Holder, Signatory or Delegated User;
 - (b) transfer funds between linked/Designated bank Accounts;
 - (c) share your account details (BSB and Account Number) via SMS, email or any other sharing medium supported by the Mobile Device. However, by sharing your account details with third parties you are potentially making your account more vulnerable to unauthorised transactions against your account, including EFT deposit and direct debit. making BPAY payments; and
 - (d) making payments to accounts that are not linked to your Account (such as accounts held with other financial institutions);
 - (e) obtaining Account information, such as Account balances, pending transactions and transaction history;
 - (f) updating personal details such as email and address;
 - (g) card management including set PIN and report lost or stolen card;
 - (h) updating statement preference;
 - (i) viewing and retrieving eStatements; and
 - (j) multi-to-sign payment authorisations.
2. Not all Online Banking Services and features are available within the BOQ Specialist Mobile App.
3. We may impose limits on your use of the BOQ Specialist Mobile App, including daily limits on withdrawals. Details of the limits we impose are set out in the applicable Other Terms.
4. If you forget or misplace your Mobile App PIN the User will have to re- register for the BOQ Specialist Mobile App as they did the first time they logged into the BOQ Specialist Mobile App on their Mobile Device.
5. Each time you use the BOQ Specialist Mobile App to access the Online Banking Service, this Part C2 and the other terms and conditions for Online Banking apply.
6. If there is any inconsistency between this Part C2 and the other terms and conditions for Online Banking, Part C2 shall prevail.

7. The BOQ Specialist Mobile App is not a stand-alone product. To Access the BOQ Specialist Mobile App you first need to download and install the BOQ Specialist Mobile App from selected digital media stores onto your Mobile Device.

8. In order to use the BOQ Specialist Mobile App you need to be a registered User of Online Banking.

9. To register the BOQ Specialist Mobile App you will be required to enter your Client Number, Online Banking Password and the six digit security code generated by your Symantec Credential into the BOQ Specialist Mobile App which you have downloaded on your mobile device. You will need to set a four digit Mobile App PIN which will then be used to access the BOQ Specialist Mobile App and authorise transactions through the BOQ Specialist Mobile App.

10. BOQ Specialist does not guarantee that the BOQ Specialist Mobile App will work on your Mobile Device, or that the BOQ Specialist Mobile App will be free from errors, flaws or bugs. BOQ Specialist is not responsible for any cost (including any internet or telephone connection charges), loss or damage which may arise from your use or attempted use of the BOQ Specialist Mobile App. However, this will not prevent BOQ Specialist from being liable where loss or damage is caused by us or our employees, agents or appointed receivers acting negligently or fraudulently or our or their mistake or wilful misconduct.

11. If you travel outside of Australia you may still have access to the Mobile Banking service. You should check with your telephone communications provider that your mobile device will be able to use relevant network in those countries in which you are travelling. BOQ Specialist is not liable for any additional costs you incur.

12. Any conditions of use and charges relating to your Mobile Device are your responsibility. "Balance Peek" is a feature available on the BOQ Specialist Mobile App. When this is set up, the User can view account balances at a glance without logging into the BOQ Specialist Mobile App.

13. The BOQ Specialist Mobile App will display Accounts from all entities that the User is a Signatory or Delegated User to.

14. You can install and register on the BOQ Specialist Mobile App on up to five Mobile Devices with one Client Number. We recommend only being logged in on one session of the Mobile App at any one time. If you are no longer in possession of one or more of your Mobile Devices, you should remove them from your devices list from the "Setting" menu, or by calling BOQ Specialist Client Services 1300 160 160.

15. If you lose your Mobile Device you can call us on 1300 160 160 (or +61 2 9293 2121 if calling from overseas).

16. Using Touch ID

(A) If you have the BOQ Specialist Mobile App installed on a Mobile Device that has Touch ID available, you will be able to turn on Touch ID access for the BOQ Specialist Mobile App. Turning on Touch ID for the BOQ Specialist Mobile App means that you can access the App using your fingerprint instead of your PIN or password.

(B) You must not turn on Touch ID access for the BOQ Specialist Mobile App if you have

any fingerprints stored on your device other than your own. If, after turning on Touch ID, you allow other people to use their fingerprints on your device, you must first turn off Touch ID access for the BOQ Specialist Mobile App.

(C) If you do allow anyone else's fingerprints to be stored on your device (despite this being against these terms and conditions):

(i) They'll be able to access your Accounts and considered authorised to do so;
and

(ii) You will be responsible for their transactions.

(D) Touch ID access for the BOQ Specialist Mobile App can only be turned on if it is available on your Mobile Device and has been enabled by you on your device. Touch ID is technology provided by a third party service provider and accordingly BOQ Specialist are not responsible:

(i) For any malfunction in Touch ID;

(ii) If Apple makes any changes to its Touch ID technology that impacts the way you access the BOQ Specialist Mobile App.

You will still be able to access the BOQ Specialist Mobile App using your PIN or password.

(E) If you choose to use Touch ID access for the BOQ Specialist Mobile App, you will still need your PIN and must set and protect your PIN in the manner outlined in these Terms and Conditions.

17. Using FACE ID or Android facial recognition

(A) If you have the BOQ Specialist Mobile App installed on a Mobile Device that has FACE ID or Android facial recognition, you will be able to turn on FACE ID or Android facial recognition access for the BOQ Specialist Mobile App. Turning on FACE ID or Android facial recognition for the BOQ Specialist Mobile App means that you can access the App using facial recognition instead of your PIN.

(B) You must not turn on FACE ID or Android facial recognition access for the BOQ Specialist Mobile App if FACE ID or Android facial recognition on your device contains facial recognition data other than your own. If, after turning on FACE ID or Android facial recognition, you allow other people to store their FACE ID or Android facial recognition data on your device, you must first turn off FACE ID or Android facial recognition access for the BOQ Specialist Mobile App.

(C) If you do allow anyone else's FACE ID or Android facial recognition data to be stored on your Mobile Device (despite this being against these terms and conditions):

(i) They'll be able to access your Accounts and considered authorised to do so;
and

(ii) You will be responsible for their transactions.

(D) FACE ID and Android facial recognition access for the BOQ Specialist Mobile App can only be turned on if it is available on your Mobile Device and has been enabled by you

on your device. FACE ID and Android facial recognition technology is provided by a third party service provider and accordingly BOQ Specialist are not responsible:

- (i) For any malfunction in FACE ID or Android facial recognition;
- (ii) If Apple makes any changes to its FACE ID technology that impacts the way you access the BOQ Specialist Mobile App.
- (iii) If Android makes any changes to its Android facial recognition technology that impacts the way you access the BOQ Specialist Mobile App.

You will still be able to access the BOQ Specialist Mobile App using your PIN or password.

(E) If you choose to use FACE ID or Android facial recognition access for the BOQ Specialist Mobile App, you will still need your PIN and must set and protect your PIN in the manner outlined in these Terms and Conditions.

(F) You also acknowledge that your use of FACE ID or Android facial recognition is subject to the terms and conditions set forth by Apple or your Android Phone provider and/or their affiliates in respect to the use of FACE ID or Android facial recognition, which will not change or override these terms and conditions.

(G) You must keep your Mobile Device safe (including ensuring that the device is not modified contrary to the software or hardware guidelines of the manufacturer). Devices modified contrary to the software or hardware guidelines of a manufacturer, including by disabling hardware or software controls, (commonly referred to as "jailbreaking", "rooting", "unlocking the bootloader" or using a debugging interface in respect of the device), are not eligible to be used for accessing the BOQ Specialist Mobile App under these term and conditions. You acknowledge and agree that the use of a modified device to use your BOQ Specialist Application is expressly prohibited, constitutes a violation of these terms and conditions, and is grounds for us to deny your access to your BOQ Specialist Mobile App.

18. Check the transaction details when using the BOQ Specialist Mobile App

(A) Please ensure you enter the correct recipient or payee details or your payment may be unsuccessful and/or you may not be able to recover a payment made to an incorrect recipient.

(B) Unless it is a scheduled payment (see Part A clause 7.3 and Part B clause 5.2), you cannot delete or cancel a BOQ Specialist Mobile App payment once it has been made.

(C) You are responsible for entering the correct recipient details when sharing information in the App via email, SMS or any other third party App installed on your Mobile Device.

Part D

Symantec Identity Protection End User Agreement

NOTE! YOU WILL CONCLUDE A LEGALLY BINDING AGREEMENT WITH THE ISSUER OF THE CREDENTIAL IF YOU CLICK "I ACCEPT" OR DOWNLOAD OR USE THE CREDENTIAL. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT CLICK "I ACCEPT" AND DO NOT DOWNLOAD OR USE THE CREDENTIAL.

~Functions and Limitations of VIP Network and Credentials~

You acknowledge the following:

Review VIP Policy. You have reviewed and understood the VIP Policy (available at www.broadcom.com/company/legal/licensing or at request), which further explains and defines some of the terms used in this Agreement.

Limited Functionality of Credentials. You understand that a VIP Credential (for example, a digital certificate or token) is intended to help you authenticate yourself to VIP Network participants (for example, participating online merchants, banks and payment providers) and increase the level of security of your web transactions with these entities. The VIP participants will use the VIP Credential to verify with a higher degree of certainty, albeit not complete security that you are indeed who you say you are. But the VIP Credential is not failproof nor can it be used as a substitute for official proof of your identity.

Security Risks. You understand that as there are inherent security risks on the Internet, you must carefully consider the degree to which you choose to rely on your VIP Credential.

Contract Parties. You understand that this Agreement is between you and the Credential Issuer. Symantec operates the infrastructure to support the use of VIP Credentials across the VIP Network. The Issuer from which you Applied for your Credential has contracted with Symantec to deliver the Credential to you.

Data Privacy. Credential Issuer, Symantec and VIP Network participants will process, share and transmit your personal data through the Internet, worldwide, to authenticate you in the context of transactions you conduct with VIP Network participants and for purposes of administering the VIP Network.

~Terms and Conditions of Use~

You agree to the following and shall be held liable if you act in contradiction of these rules:

1. Comply with this Agreement, the VIP Policy and all laws. You must use the VIP Credential and any related service only in accordance with this Agreement, the VIP Policy (available at www.broadcom.com/company/legal/licensing or at request) and all applicable laws and regulations.
2. Accurate Information. You agree to provide accurate information and to provide all information reasonably requested by Symantec or the Credential Issuer.

3. Your Security Obligations. You will maintain secure possession of the VIP Credential and promptly notify the Credential Issuer if you lose possession for any reason (for example, if you change your mobile phone containing the VIP Credential or if you lose the token or hardware device which stores the VIP Credential). You may not let someone else use your VIP Credential.

4. Termination. Symantec and the Issuer may revoke your VIP Credential, each at its own discretion, if you breach this Agreement or if you compromise the security or integrity of the VIP Network.

~Disclaimers~

If you are a consumer as defined in section 12BC of the Australian Securities and Investments Commission Act 2001, Credential Issuer's and Symantec's liability to you will be as set out in clause 18.1 of Part A of these terms and conditions (and all references to " BOQ Specialist" in that clause shall be read as " BOQ Specialist and Symantec"). In all other instances, in light of the limited functionality of the VIP Credentials and VIP Network as defined in this Agreement, Credential Issuer and Symantec disclaim all warranties and representations (Credentials are issued "AS IS"!) and limit their liability for any losses or damages (whether based on contract, tort, statute or any other legal theory) related to your use of the VIP Credential to the fullest extent possible under applicable law. Your sole and exclusive remedy for any malfunction, deficiency or other dissatisfaction related to VIP Credentials is a claim against the Credential Issuer to issue a replacement VIP Credential.