ELECTRONIC BANKING SAVE, SPEND & CMA

TERMS & CONDITIONS

EFFECTIVE 2 MARCH 2022

CONTENTS

These terms regulate how you transact electronically on your Volt accounts. Please read them carefully. They will help you get the best out of your accounts with Volt and the best out of us. Some words, used in the terms, are explained at the end of these terms at clause 32.

1. EPAYMENTS CODE

The ePayments Code sets out rules for the way electronic transactions must be managed. All transactions you can make on your account are electronic transactions.

The ePayments Code:

- requires detailed terms about electronic transactions. There is a lot to it, but it is worth reading so you know your rights and responsibilities; and
- sets out rules for determining who pays for electronic transactions you did not authorise. Sometimes, you can be responsible for all or part of an unauthorised electronic transaction.

We:

- promise to comply with the ePayments Code for all transactions covered by the Code; and
- will work out who is responsible for unauthorised transactions and liability in accordance with the ePayments Code.

2. WHAT IS AN UNAUTHORISED TRANSACTION?

Just to make it clear, any transaction is authorised by you if:

- you make the transaction; or
- it is performed by anyone with your authority, knowledge or consent, even if the transaction was for the wrong amount or was made to the wrong person. Your consent to a transaction may be given by you directly or your consent may be clear from your conduct.

Transactions not made:

- by you; or
- with your authority, knowledge or consent,

are unauthorised transactions.

3. ACCESSING INFORMATION AND FUNCTIONALITY

NOTE: You cannot deposit funds by cash or cheque.

We are a digital bank. You cannot make transactions on your account by phoning us. We do not issue or accept deposits of cheques, bank cheques, cash or money orders into your account.

Access

With a Volt Account you can make transactions from your mobile or desktop device at any time to:

- send payments from your Volt accounts to other bank accounts by using the username we give you and the passcode you choose (Pay Anyone);
- make a BPAY® payment for CMA and Spend;
- view or update your residential address;
- view your mobile number or email address;
- change your passcode;
- check the current interest rate on your account;
- add your TFN or TIN; or
- view your transaction history.

A daily transaction limit applies to Pay Anyone transactions. Those limits are set out in your Volt Product Terms.

Those limits may change. Information regarding daily transaction limits can also be found at voltbank.com.au/help.

BPAY® PAYMENTS

NOTE: you cannot cancel BPAY® payments or request chargebacks.

We are a member of the BPAY® scheme. We will tell you if we are no longer a member. The following terms apply if you use BPAY® when making a payment:

By using BPAY® you can make payments or transfer money from your CMA or Spend account (but not Save). If you use BPAY ® to pay a bill, that bill should tell you the Biller number and customer number you must use to make the payment. Please take care when you enter the details of a BPAY® payment you wish to make. We may not be able to

recover BPAY® payments, made to the wrong account, or overpayments.

You cannot cancel a BPAY® payment on the day that you asked us to make that payment.

Usually, if you make a BPAY® payment before our cut off time (4:00 PM Sydney time) on a business day, we process the payment that day and the Biller receives it that day. We process other BPAY® payments on the next business day.

Sometimes it takes longer to complete a BPAY® payment, like if there is a public holiday after the day you make the payment or the Biller or its financial institution does not process the transaction as the BPAY® scheme rules require.

Sometimes, access to your account will not be available. That could be due to routine maintenance or if we have a security concern we need to investigate. We will try to give you notice of scheduled maintenance via email or SMS or via the Volt app or Partner app. We may not be able to give you notice of emergency maintenance.

■ BPAY® MISTAKEN PAYMENTS, UNAUTHORISED TRANSACTIONS, AND FRAUD

You should notify us immediately if you become aware:

- that you may have made a mistake when instructing us to make a BPAY® payment;
- if you did not authorise a payment that has been made from your account; or.
- if you think that you have been fraudulently induced to make a payment.

The longer you delay in telling us the more difficult it may be to assist.

If you instruct us to make a payment and you later discover that the amount you told us to pay was less than the amount you needed to pay, you can simply make another payment for the difference between the amount actually paid to a biller and the amount you needed to pay.

■ MISTAKE

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

■ UNAUTHORISED

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

- we cannot recover that amount within 20 business days of us attempting to do so that from the person who received it; and
- the payment was made as a result of a payment direction which did not comply with our prescribed security procedures for such payment directions

■ FRAUD

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

■ INDEMNITY

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

- did not observe any of your obligations under the terms and conditions in this section; or
- acted negligently or fraudulently in connection with these terms.

■ CONSENT

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

erroneous BPAY® payment does not or will not constitute under any circumstance part or whole satisfaction of any underlying debt owed between the payer and their biller.

- When a biller cannot process a BPAY payment

  If we are advised that your BPAY payment cannot be processed by a biller, we will:

  - advise you of this
  - credit your account with the amount of the BPAY payment; and
  - if you ask us to do so, take all reasonable steps to assist you in making the BPAY payment as quickly as possible.

- Consequential damage

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

- Suspension

  We may suspend your right to participate in the BPAY scheme at any time acting reasonably.

  The circumstances in which we may suspend your right to participate in the BPAY scheme include if you or anyone acting on your behalf is suspected of being fraudulent.

- No "chargebacks"*

  Except where a payment is a mistaken payment, an unauthorised payment, or a fraudulent payment as referred to above, payments are irrevocable. No refunds will be provided through BPAY payments where you have a dispute with the Biller about any goods or services you may have agreed to acquire from the Biller. Any dispute must be resolved with the Biller.

IMPORTANT
Even where your payment has been made using a debit card, no "chargeback" rights will be available for BPAY payments.

4. ▼ VOLT SPEND

Clauses 4 and 5 apply only to Volt Spend

NOTE: Some third parties may not permit direct debits.

- Volt Spend

With a Volt Spend account you will be issued with a debit card and can make transactions:

- by using your debit card and PIN at ATMs or POS terminals until the expiry date on the card;
- using your debit card to make contactless payments at merchants that accept those payments;
- by arranging direct debits (if permitted) from your account.
- With a Volt Spend account, you can also make Direct Entry payments and direct debits (if permitted) and transfers between accounts in your name
- Sometimes if you have established an account through a third party that third party will not allow you to establish direct debits on your account.

5. ▼ MASTERCARD® DEBIT CARD

You will receive a debit card to withdraw money from your Volt Spend account, or to make purchases. You must activate your card before you can use it.

The debit card may be used to purchase goods or services from merchants or withdraw cash in the following ways:

- By ATM in Australia or overseas wherever a Mastercard logo is displayed. You can withdraw cash from your Volt Spend by pressing the 'credit' button and entering your PIN;
- By holding your debit card in front of any contactless terminal and waiting for the transaction to be confirmed. In Australia, there is no need to sign or enter a PIN for purchases up to $100. At merchants overseas you may need to sign or enter a PIN for small value transactions.
- Online – by using the debit card number and expiry date on your card as well as the card verification number.
- Over the phone – by quoting the debit card number and expiry date on your card and quoting the card verification number on the back.

Your PIN may be a 4-digit number that you set yourself in the

Volt app. You have the option of changing your PIN at any time using the Volt app.

Debit cards are only to be used until the expiry date. Just prior to expiry we will issue you with a replacement card and you should ensure that, once received, you destroy the old one by cutting it into several pieces and disposing of it securely.

- Loss, theft or misuse of a Debit Card, PIN or passcode.

You must immediately notify us if your debit card, PIN or passcode record is lost, stolen or misused, or you suspect that unauthorised transactions have been made on any account. This will enable us to put a stop on your debit card straight away preventing or minimising losses resulting from unauthorised transactions and your potential liability for such losses.

You must report it to us by phoning 13 VOLT (13 8658), or emailing customercare@voltbank.com.au as soon as you can.

- Locking or Cancelling your Debit Card

Contact Customer Care using live chat within the Volt app or contacting us at customercare@voltbank.com.au or by phoning us on 13 VOLT (13 8658) during our standard business hours if you would like to temporarily suspend, unsuspend or lock your debit card. If your debit card is damaged and you need a new one Customer Care can also assist you by issuing you with a new one using the same card details. You may continue to use the damaged debit card until you get a new one.

If you would like to cancel and replace a debit card that has been lost or stolen contact Customer Care at customercare@voltbank.com.au or phone us on 13 VOLT (13 8658) during our standard business hours.

For lost and stolen debit cards your debit card will be automatically cancelled once you have notified us and a new one with new details will be sent to you in the mail. Please note that once a lost or stolen debit card is cancelled you won't be able to use that debit card to make purchases or withdraw from an ATM until you get a replacement, however you will be able to continue to use the card details if they were added to Apple Pay / Google Pay prior to being cancelled.

We may also cancel a debit card at any time, to protect you or us from fraud or other losses, to manage regulatory risk, or for any other reason determined by us acting reasonably. If your debit card is cancelled, you must stop using it and destroy it by immediately cutting it into several pieces and disposing of them securely. If you close your accounts or cancel the debit card, as the account holder, you will remain liable for transactions made using the debit card linked to your account:

- prior to or after its cancellation or closure of the accounts; or
- using the card number for mail, online, phone and recurring transactions which have not been cancelled prior to termination.

- Card reissue

We may issue a new debit card to you at any time and just prior to the debit card expiry on the same terms and conditions. We have the right to refuse to reissue a debit card if we choose.

- Authorising debit card transactions

When you use a debit card you may need to seek authorisation from us. We may choose not to authorise a proposed transaction at any time.

Reasons why we might refuse to authorise the transaction include:

- the card has expired or is otherwise invalid;
- your account does not have sufficient funds in it to cover the transaction amount;
- acting reasonably, we consider the transaction may be fraudulent;
- based on information available to us, we consider the transaction may affect the security of your account or our systems;
- we reasonably suspect any other unlawful activity in relation to the transaction;
- we reasonably suspect the transaction is not authorised;
- you or we have closed the account;
- you have not complied with our terms and conditions;
- we reasonably believe it could cause us (or any affiliate) to breach a foreign or domestic law, including our foreign reporting obligations.

- Daily limits

  To help protect an account from fraudulent card transactions, we have set default limits on individual and daily withdrawal and card transaction amounts. You can ask us to change the daily withdrawal limits that apply to your account. We do not have to agree but if we do, those limits will apply from the time we process your request.

  Note: the daily limits are expressed in Australian Dollars. If you transact in a foreign currency, the limit applied will be the Australian Dollar equivalent.

NOTE: Merchant authorisations may reduce available credit.

- Limits set by other providers

  Please note that merchants or other providers of facilities may impose additional limits.

  If we authorise a transaction, we will reduce the amount in your account by the amount of the authorisation. However, some merchants, such as hotels and car rental agencies, may request confirmation that your account has sufficient available balance to meet the estimated cost of the goods and services they will supply prior to the supply of those goods or services. When that occurs the request will be treated as an authorisation even if the funds have not yet been used. That means that even though the balance of your account is a certain amount, the amount we permit you to withdraw will be reduced pending the supply of the goods and services. When the goods and services have been supplied, the merchants may request a subsequent authorisation for the actual costs. You should ensure that prior to the merchant doing this the original authorisation is cancelled to avoid the available balance being reduced twice.

  As debit card transactions may take some weeks to be processed and debited to your account please take that into account when checking your balance as the available balance in your account may be less than the actual balance shown whenever you obtain a statement, mini transaction history or a balance of your account.

- How Mastercard processes foreign currency transactions

  When a Mastercard debit card is used to make foreign currency transactions on your account, the transaction is converted into Australian dollars by Mastercard using:

  - a rate Mastercard selects from the range of rates available to it in wholesale currency markets for the date on which Mastercard processes the transaction. The rate Mastercard selects may vary from the rate Mastercard receives itself; or
  - a rate a government requires Mastercard to apply to the conversion as at the date the transaction is processed.

  Mastercard may convert a foreign currency transaction into US dollars prior to converting it into Australian dollars.

- Dynamic currency conversion

  When you make a purchase or withdraw cash from your account in a country other than Australia, the merchant or ATM provider may give you the option to complete the transaction in a different currency, usually in Australian Dollars. If you accept this offer, the merchant or the ATM operator will perform the foreign exchange conversion on the transaction on your behalf at an exchange rate they determine. This is also referred to as 'Dynamic Currency Conversion'. **We do not determine this exchange rate and it may not be favourable to you.**

- What to do if you want to dispute a debit card transaction

  If you don't recognise a transaction, you should contact us as soon as possible. Please email us at customercare@voltbank.com.au or contact us by Live Chat if using the Volt app or phoning us on 13 VOLT (13 8658) during our standard business hours.

  We may ask you to provide information to support your dispute. We must comply with card scheme rules which set out dispute procedures and notification timeframes. If you do not notify us promptly, we may not be able to investigate your dispute.

  In some circumstances, card scheme rules allow us to charge a transaction on the account back to the merchant with whom you made the transaction. This is known as a chargeback. If it is available, we will claim a chargeback right for a transaction on your account if you ask us to do so, and you give us the information and material we require to support a chargeback. Otherwise any chargeback right we have may be lost. The timeframe for disputing a transaction may not apply where the ePayments Code applies.

- Chargebacks

In some cases under the Mastercard rules we can charge a disputed transaction back to the merchant. This is called a chargeback. Not all transactions have chargeback rights, for example, BPAY® transactions.

Chargeback rights only apply if the transaction was processed using your debit card.

If you dispute a transaction and you want a chargeback, you must report this to us as soon as possible and give us all the information that we request to support a chargeback request. You need to make the request to us within 30 days after the date of the statement which includes the transaction (this may not apply for unauthorised transactions covered by the ePayments Code). We will then make the chargeback request if we are allowed to under the Mastercard rules. The request may not be successful.

6. ▼ DEPOSITS

NOTE: You cannot deposit cash or cheques into Volt accounts.

You can deposit money into your account through Pay Anyone from another account held with another financial situation. You will need to use or give the payer our BSB (Bank/State/Branch, if you were wondering) and your account number. Our BSB is 517-000. Also, you can transfer money into your account from any other account you hold with Volt Bank.

A transfer into an account held by you with Volt through the Pay Anyone facility forms part of the available balance of that account only after it is cleared.

It may take some time to clear a transfer from another financial institution depending on the time of day you instruct the other financial institution and whether the transfer is made on a business day.

You cannot deposit money into your account by cheque or cash.

- Minimum and maximum limits

We may apply limits on the minimum and maximum amount for transactions and balances on an account and vary those limits from time to time. These limits may apply to your opening and ongoing balance.

7. ▼ WITHDRAWALS AND PAYMENTS

You can withdraw money or make payments from your account by:

- giving someone a direct debit request (if permitted) to draw payments regularly from your account on the terms in that request.
- transferring funds using Pay Anyone or NPP Payment to transfer money to any other account held with a financial institution in Australia. You will need the BSB and number of the account, to which you wish to make the transfer or payment or PayID (for NPP Payments).
- using BPAY (for Volt Spend and CMA only) to make payments or transfer money. If you use BPAY to pay a bill, that bill should tell you the Biller number and customer number you must use to make that payment.

Scheduled and recurring payments are not available at this time.

Please take care when you enter the details of the other account. We will warn you to check the payment details you entered before you complete a Pay Anyone or NPP transaction and in time for you to cancel the transaction.

We may be able to recover transactions made to the wrong account. More on that in clause 9.

Be aware that if a payment is made by you on a day that is not a business day, we will process the payment on the next business day.

- When we do not process a withdrawal or payment

We may decide not to process a withdrawal or payment from your account if:

- the available balance is not enough to cover the transaction
- the amount is in excess of the daily limit
- based on information available to us, we consider the transaction:
  - may be a fraudulent request
  - may affect the security of your account or our systems

- we are aware or suspect that the security of a passcode has been breached
- would breach these terms

8. STOPPING TRANSACTIONS

We can't stop processed transactions.

Each time you make a transaction on your account, you direct us to process that transaction.

9. MISTAKEN PAYMENTS DIRECT ENTRY ('PAY ANYONE') FACILITY

- Reporting

If you make a Pay Anyone payment to the wrong person, please phone us on 13 VOLT (13 8658) for the cost of a local call. We will acknowledge your report and give you a reference number, if you need to follow us up. We encourage you to report any payment you made by mistake as soon as possible after you work out there was a mistake. The earlier the report, the better the chance of recovery.

If you report a mistaken payment to us, we will investigate. You consent to us disclosing this information to other financial institutions in order to request a return of your funds.

If it looks to us like the payment was not by mistake or did not occur, we will take no further action.

If it looks to us like the payment occurred and was by mistake, we will ask the financial institution (other financial institution), to return the payment to us.

We will report to you about our dealings with the other financial institution. We cannot promise that the other financial institution will return the money to us. We will do our best.

If a mistaken payment is returned to us, we will credit your account. If you no longer hold that account, we will contact you and you can tell us how you want us to pay you the money we recover.

One way or another, we will tell you in writing about the outcome of our investigations within 30 business days after your report. We will give you the opportunity to dispute our decision, if you are not happy with it.

We will not ask you to deal with the other financial institution to sort out your complaint.

- Mistaken Payment rights

The ePayments Code includes detailed rules on when another financial institution must return a mistaken payment. There are more details below.

- Report within 10 business days

The other financial institution must return the amount of a mistaken payment if:

- you report to us within 10 business days after the payment was made
- it looks to the other financial institution that the payment was a mistake; and
- there are sufficient credit funds in the account of the person (the enriched person) who received the payment for the money to be returned.

- Report after 10 business days, but within seven months

If you report the mistaken payment to us after more than 10 business days, but within seven months, and:

- it looks to the other financial institution that the payment was a mistake
- there are sufficient credit funds in the enriched person's account
- then the other financial institution must:
- prevent the enriched person from withdrawing funds from their account for up to 10 business days
- notify the enriched person that it will return the mistaken payment to us, unless the enriched person can prove that they are entitled to the payment.

- Later reports

If you report the mistaken payment to us more than seven months after the payment was made, and:

- it looks to the other financial institution that the payment was a mistake
- there are sufficient credit funds in the account of the enriched person for the money to be returned

The other financial institution must seek the person's consent to return the money to us. The person does not need to

consent. You may be able to take other action available directly against the enriched person to recover the mistaken payment.

- Mistaken payments to you

Where:

- we are satisfied that a payment made to your account is a mistaken payment; and
- you have sufficient credit funds in your account to the value of that payment; and
- the mistaken payment is reported 7 months or less after the payment; and
- for mistaken payments reported between 10 business days and 7 months of the payment, you don't establish that you are entitled to the payment within 10 business days;
- we will, without your consent, deduct from your account an amount equal to that mistaken payment and send that amount to the financial institution of the payer.

If there are insufficient funds in your account, you must co-operate with us to facilitate payment by you of an amount of the mistaken payment to the payer.

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

10. ▼ BALANCES AND TRANSACTION RECORDS

You must provide us with a description of the transaction at the time you make that transaction. We record those details of the transaction and give you a receipt number as a record of that transaction for you to refer to in the Volt app or Partner app as and when you need it.

We add deposits to your account balance. We deduct withdrawals from your account balance.

11. ▼ FEES AND CHARGES

Volt does not charge you any fees for opening and operating an account with us. You may have to pay fees and charges on transactions you make on your account or when using your debit card. Please check your account terms for any fees that may be payable.

You may incur charges from your network service provider for using any electronic equipment for accessing your account. Those charges are your responsibility. Please raise any matters regarding those charges with your network service provider.

12. ▼ SECURITY REQUIREMENTS

- Two–factor authentication

To assist in keeping your account secure, we may require two–factor authentication for some dealings you have with us. Examples include when you update your residential address, the first time you make a payment using the Volt app, and when you reset your passcode. In many cases, the two–factor authentication occurs without requiring any action from you. However, in some cases, we may require you to verify your email and phone number to confirm the changes or instructions that you have requested.

If you do your banking on your mobile device, and your mobile device allows you to control access to it using biometric information, like a fingerprint or facial data, we may allow you to use this information to log into your account instead of using a username and passcode.

Volt does not collect or store biometric information stored on your device. If you wish to sign in using biometric information, please ensure that only your own biometric information is stored on your mobile device. Otherwise, another person could transact on your account using their biometric information.

- Third Parties

Generally, Volt does not allow other people to operate on your account. If another person has access to your account using your details we will treat those transactions as having been authorised by you and conducted with your knowledge and consent.

Please take steps to ensure if using a mobile device or computer that they are secure. Also, it is important to ensure that any biometric information used in connection with your device, is always secure.

- Suspending your account

  If we suspect the security of your biometric information or device is breached, we may need to suspend your banking access or restrict certain features on your account to protect your account.

- Choosing your passcode

  You need your username and passcode to transact on your account when using the Volt app and the Partner app. When using the Volt app your username is the email address you give us when you applied to open your account. You get to choose your own passcode. You can change or reset your passcode through the Volt app, or if through the Partner app, as directed by the Third Party Partner.

  When you use the Volt app or Partner app to transact on your account, you may also choose to use your biometric information to login to your account, instead of your passcode.

  When using passcodes you must ensure that the passcodes are not easy to guess. You must not choose a passcode that:
  - is part of your mobile number;
  - is numeric and represents your birth date; or
  - contains single or consecutive digits (e.g. 111111, or 123456)

  If you choose one of those passcodes, you may be responsible for unauthorised transactions by use of that passcode on your account.

  We will tell you if there are any other passcode requirements at the time you choose the passcode.

  It is a good idea to change your passcode occasionally.

- Keeping your passcode secure

  You must make a reasonable attempt to protect the security of your passcode. Please keep that in mind if you decide to keep a record of your passcode. The more secure it is, the less likely that unauthorised transactions will occur on your account.

  Do not disclose your passcode to anyone, including a family member or friend.

  If you are extremely careless in not protecting the security of your passcode, you may be liable for unauthorised transactions. One example of being extremely careless is keeping a record of your passcode in a diary under the heading "Volt passcode". There are other examples. Please make a good effort to keep your passcode secure.

- Personal use only

  Your passcode is for your use or for someone you have authorised . You must not disclose it to any other person, even if that other person is a family member or a friend. We will never ask you to disclose your passcode to us.

13. REPORTING SECURITY BREACHES AND UNAUTHORISED TRANSACTIONS

If:

- you lose your passcode;
- someone steals your passcode;
- you know, or you suspect that, your account is no longer secure;
- you believe someone else may have used their own biometric information to gain access to your account; or
- you are aware of unauthorised transactions on your account,

you must report it to us by phoning 13 VOLT (13 8658) for no more than the cost of a local phone call, or emailing customercare@voltbank.com.au as soon as you can.

We will acknowledge receiving your report and give you a reference number, if you need to follow us up.

You are not responsible for any loss arising from unauthorised transactions that occur when our phone service is not available, as long as you report to us within a reasonable time of our phone service becoming available again. If you cannot get through to our phone number immediately, please leave a message or phone us back or email us at customercare@voltbank.com.au.

When you make a report, we may:
- suspend your account until we are satisfied that your account is secure. More on suspending your account at clause 12.
- ask you to create a new passcode

When you make a report, we may:

- suspend your account until we are satisfied that your

account is secure. More on suspending your account at clause 13.
- ask you to create a new passcode

14. WHEN YOU'RE NOT RESPONSIBLE FOR UNAUTHORISED TRANSACTIONS

You are not responsible for loss from an unauthorised transaction if:

- that loss was caused by the fraud or negligence of our employees or agents;
- that loss was caused by a transaction being debited more than once to your account by mistake
- that loss was caused by:
- a passcode that is forged, faulty, expired or cancelled
- a transaction requiring the use of a passcode that occurred before you created that passcode; or
- a transaction being debited more than once to your account by mistake;
- it is clear you did not contribute to the loss
- the transaction occurred after we find out that your account is no longer secure

15. WHEN YOU'RE RESPONSIBLE FOR UNAUTHORISED TRANSACTIONS

NOTE: In limited circumstances, you may be liable for some or all of an unauthorised transaction.

■ Proof

Whenever this term refers to us having to prove an event, it means we have to prove that event on the "balance of probability". That means the event is more probable than not.

■ Fraud and security requirement breaches

If we can prove that you or an authorised person contributed to a loss from unauthorised transactions due to fraud, or breaching the security requirements in clause 11, you are responsible for losses that occur before you report to us that your passcode or account is no longer secure.

Clause 13 sets out how you can report those events to us.

■ Reporting delays

If we can prove that you contributed to losses from unauthorised transactions by unreasonably delaying reporting that the security of a passcode or your account is breached under clause 13, you are responsible for the losses that occur between:

- when you became aware of the security breach; and
- when we were informed of that security breach

We consider all circumstances to decide whether you unreasonably delayed reporting a security breach to us.

16. WHEN YOU CONTRIBUTE TO LOSSES FROM UNAUTHORISED TRANSACTIONS

If there are losses from unauthorised transactions that:

- required the use of a passcode; and
- are not covered by clause 14 or clause 15,

you are responsible for the lowest of:

- $150;
- the sum of the available balances on accounts you can access using your passcode; and
- the actual loss at the time you report to us that the security of your passcode is breached

17. LIMIT ON YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS

In any case, you're not responsible for losses on your account from unauthorised transactions:

- on any one day that exceeds the daily transaction limit on your account under your account terms;
- in any period that exceeds any transaction limit for that period on your account;
- exceeding your available balance; or
- on any account that we have not agreed with you to be accessed using the passcode used to perform the unauthorised transaction.

Please remember that you're not responsible for any loss set out in clause 14.

18. SHARED NETWORK

We may participate with others in shared electronic payments networks. BPAY® is an example of a shared electronic payments network. There are others.

Any other network participant's conduct does not excuse us from any obligation we owe you.

We will not ask you to:

- raise a complaint about the processing of a transaction with another network participant; or
- have that other network participant investigate your complaint or a dispute about a transaction

19. GOOGLE® PAY TERMS AND CONDITIONS CLAUSES 19 AND 20 APPLY ONLY TO VOLT SPEND

Google Pay is for android users.

By adding your Debit Card to Google Pay you agree to the terms in this section which will also apply to any Device you link to Google Pay and your Account.

To download the Google Pay App visit Google Play or the app store.

- Google Pay

Google Pay is a service provided by Google and therefore we are not responsible for use of the service such as costs associated with Google Pay or it being unavailable, or the failure of third-party merchants to accept payments using Google Pay. By using Google Pay you agree that:

- Google can provide us with certain information relating to your use of Google Pay including your Device details, location and personal information. Further information about how Volt handles that data is available in our Privacy Policy available at: voltbank.com.au/privacy-policy.html
- We can provide Google with certain information to allow Google and its service providers to operate Google Pay, detect and address fraud, or improve and promote Google Pay and other Google products and services and comply with any laws that apply to Google Pay. Please note that Google may store this information outside Australia. Please refer to Google's Privacy Policy at https://policies.google.com/privacy for any further information about how Google handles your information.
- We and Google may provide certain information to Mastercard to operate Google Pay and to comply with any laws. Mastercard will handle any personal information in accordance with their privacy policy, which can be found by searching "Mastercard privacy" at mastercard.com.au. If you do not agree to your information being disclosed or used in this manner you should not add your Debit Card to Google Pay.

- Verification

For your security we require you to be verified when adding a Debit Card to Google Pay. To find out how you can be verified download the Google Pay App and follow the Get Started instructions. You can also refer to the Google Pay FAQs at voltbank.com.au/faq/google.

- Google Pay Payments

When adding your Debit Card to Google Pay, your Google Pay payments will be processed by debiting the Account you have linked to your Debit Card.

- Transaction Limits

The transaction limits that apply to your Debit Card when making payments will also apply to your Device and will not change as a result of you making a payment through Google Pay. For your security when using Google Pay you may be requested to authorise a transaction by entering the security credentials you use on your Device.

- Virtual Account Number

A Virtual Account Number is used to process Google Pay Payments. For your security when you add your Debit Card details to your Device those details are replaced with a Device Account Number used by Google Pay with Mastercard. Your Device Account Number is unique for that Debit Card and will not work outside of the Google Pay App or with any other card you may have. Whenever you pay with Google Pay, it is your Device Account Number that is sent to the merchant and not your Debit Card details. The merchant will then provide you with a receipt for the payment with a partially masked Device Account Number for your additional security.

- Device

You are required to keep the Google Pay App on your Device. If it is deleted you will not receive a Google Pay Transaction Receipt for your payments. You acknowledge that deleting the Google Pay App alone will not disable Google Pay and your Device Account Number will remain on your Device. To find out how to remove your Device Account Number refer to the Google Pay FAQs at voltbank.com.au/faq/google.

- Fees and Charges

We will not charge you any additional fees for adding Google

Pay to your Debit Card or Device. You are responsible however for any third-party charges associated with the use of Google Pay (such as carrier or mobile data charges).

- Protection and liability for unauthorised transactions

You must keep your Device and security information safe and secure at all times, in the same way you would with your Debit Card and PIN. The requirements about protecting your Debit Card and PIN and liability for unauthorised transactions extends to your Device and Google Pay Payments. You must not share your Device security details or allow another person to register their biometric identifier (e.g. a fingerprint or retinal scan), as that person will be able to make Google Pay Payments for which you will be held responsible.

- Lost or Stolen Device and liability

If your Device is lost, stolen or misused you should immediately remove your Debit Card(s) from your Device. Refer to the Google Pay FAQs for how you can do this. This will mean that you can continue to use your Debit Card to make purchases. If you are unable to remove your Debit Card from your Device you should immediately notify us to suspend or cancel your Debit Card which will include your Virtual Account Number. We will not be liable for any loss or matters beyond our reasonable control (e.g. failed third party software and network providers) arising from your use of Google Pay (subject to your rights under the ePayments Code).

- Suspension or termination

NOTE: In limited circumstances, we may suspend your use of Google Pay.

We will suspend or terminate your use of Google Pay if we receive your instructions to do so. We may also suspend or terminate your use of Google Pay without notice at any time where we suspect unauthorised transactions have occurred, Google Pay is being misused, to restore the security of a system or any Debit Card or account, or if required by law. We will give you notice if your Debit Card is no longer eligible to use Google Pay.

20. ▼ APPLE® PAY TERMS AND CONDITIONS

Apple Pay is for Apple users.

By adding your Debit Card to Apple Pay you agree to the terms in this section which will also apply to any Device you link to Apple Pay and your Account. To download the Apple Pay App visit the Apple Store.

- Apple Pay

Apple Pay is a service provided by Apple and therefore we are not responsible for use of the service such as costs associated with Apple Pay being unavailable, or the failure of third-party merchants to accept payments using Apple Pay. By using Apple Pay you agree that:

- Apple can provide us with certain information relating to your use of Apple Pay including your Device details, location and personal information. Further information about how Volt handles that data is available in our Privacy Policy available at: voltbank.com.au/privacy-policy.html.
- We can provide Apple with certain information to allow Apple and its service providers to operate Apple Pay, detect and address fraud, or improve and promote Apple Pay and other Apple products and services and comply with any laws that apply to Apple Pay. Please note that Apple may store this information outside Australia. Please refer to Apple's Privacy Policy at apple.com/au/privacy for any further information about how Apply handles your information.
- We and Apple may provide certain information to Mastercard to operate Apple Pay and to comply with any laws. Mastercard will handle any personal information in accordance with their privacy policy, which can be found by searching "Mastercard privacy" at mastercard.com.au. If you do not agree to your information being disclosed or used in this manner you should not add Apple Pay to your Card.

- Verification

For your security we require you to be verified when adding a Debit Card to Apple Pay. We may use Mastercard® to verify you on our behalf. To find out how you can be verified please refer to the Apple Pay FAQs at voltbank.com.au/faq/apple.

- Choosing Debit Cards for Apple Pay

When adding your Debit Card to Apple Pay, your Apple Pay payments will be processed by debiting the Account you have linked to your Debit Card.

- Transaction Limits

The transaction limits that apply to your Debit Card will also apply to your Device and will not change as a result of you adding Apple Pay to your Debit Card. When using Apple Pay you will be requested to authorise a transaction by entering

the security credentials you use on your Device.

- Device Account Numbers

  Each time you add a Debit Card to your Device your Device will be allocated a new Device Account Number. When you use your Device for a payment the receipt the merchant will provide you with will contain a partially masked Device Account Number rather than your Debit Card number.

- Fees and Charges

  We will not charge you any additional fees for adding Apple Pay to your Debit Card or Device. You are responsible however for any third-party charges associated with the use of Apple Pay (such as carrier or mobile data charges).

- Protection and liability for unauthorised transactions

  You must keep your Device and security information safe and secure at all times, in the same way you would with your Debit Card and PIN. The requirements about protecting your Debit Card and PIN and liability for unauthorised transactions extends to your Device and Apple Pay Payments. You must not share your Device security details or allow another person to register their biometric identifier (e.g. a fingerprint or retinal scan), as that person will be able to make Apple Pay Payments for which you will be held responsible.

- Lost or Stolen Device and liability

  If your Device is lost, stolen or misused you should immediately remove your Debit Card(s) from your Device. Refer to the Apple Pay FAQs for how you can do this. This will mean that you can continue to use your Debit Card to make purchases. If you are unable to remove your Debit Card from your Device you should immediately notify us to suspend or cancel your Debit Card which will include your Device Account Number. We will not be liable for any loss or matters beyond our reasonable control (e.g. failed third party software and network providers) arising from your use of Apple Pay (subject to your rights under the ePayments Code).

- Suspension or termination

  NOTE: In limited circumstances, we may suspend your use of Apple Pay.

  We may suspend or terminate your use of Apple Pay without notice at any time where we suspect unauthorised transactions have occurred, Apple Pay is being misused, to restore the security of a system or any Debit Card or account, or if required by law. We will give you notice if your Debit Card is no longer eligible to use Apple Pay.

21. NEW PAYMENTS PLATFORM

The terms in this section will apply should you choose to make payments from your Accounts through the New Payment Platform (NPP).

NPP allows for two payment types:

- Single Credit Transfers (SCTs);and
- Osko Payments.

Currently Volt only has Single Credit Transfers (SCTs) but will be subscribing to Osko in the future. We will let you know once we have Osko functionality. In the meantime terms in this section describing Osko payments will not yet apply yet.

- Transaction Limits

  Volt transaction limits for NPP Payments will be the same as currently exist for any other types of Volt transfers.

- PayID

  You can use PayID to make SCT and Osko payments or BSB and account number.

  If you use a PayID it must be linked to one of your Volt Bank accounts through either your e-mail address or Australian mobile telephone number.

  Once you create a PayID people can use that to make a payment to your Linked Account.

  Each PayID can only be linked to one account at a time. For example, you can use your Australian mobile number and email address as the PayID for one of your Volt accounts but then you can't use the same PayID for another account at the same time. But you can have several PayIDs for that same account.

- Creating your PayID

  You can create a PayID for your Volt account when you log in to your account.

  In creating a PayID, you must confirm that:

  - you own, or are otherwise authorised to use, the PayID you choose;
  - the PayID is current, accurate and complete;
  - you are authorised to operate the account to which the

PayID relates; and
- you agree to your PayID being created in the PayID Service.

We can refuse your request to create a PayID where:

- we have not verified your identity;
- we are not satisfied that you own or are otherwise authorised to use the PayID you choose;
- we reasonably suspect that the PayID is or has been or will be used for a fraudulent purpose;
- we consider the PayID could mislead or deceive a payer into sending you NPP Payments intended for another payee, or that we otherwise deem inappropriate;
- we are required to do so by law or by the operator of the New Payments Platform; or
- the PayID is already created.

Where your attempt to create a PayID is unsuccessful, we will tell you. This may be because the PayID is already registered to someone else, or an incorrect format has been used, or the account against which it is being registered is not in scope for the PayID Service. We cannot however disclose personal information to you in connection with duplicate PayIDs.

If the PayID is already registered to you (but on another account), you may choose to transfer that PayID to your Volt account.

If the PayID is already created by someone else for less than 6 months, we will try to assist you to resolve the issue by contacting the financial institution or other entity that registered that PayID, who is then required to contact their customer who registered the PayID to establish if that customer has the right to use the PayID. If that person cannot establish that they are the rightful owner of the PayID, their financial institution is required to close that PayID. We may share with you the details of the other financial institution but can't disclose the identity of the other customer or their account details to you.

- PayID Name

When you create your PayID, we will issue you with a PayID Name which is a reasonable representation of your account name. For example if an account is held in the name of Jane Doe you can have a PayID Name like J. Doe, to ensure that the payer can confirm that they are sending the funds to the correct payee.

- Transferring your PayID to a different account with Volt or another financial institution

You can transfer your PayID to another account with us, or to an account you have with another financial institution. You can do this through the 'PayID' function in our Volt app, Partner app or as otherwise directed which means that we will temporarily lock and transfer your PayID to another account. You will not be able to use your PayID while your PayID is locked.
In transferring a PayID, you are representing that you have authority to use the PayID.

A request to transfer your PayID to another eligible account with us will generally be effective immediately.

A transfer of your PayID to another financial institution will require that other financial institution's PayID to effect the transfer.

Until the transfer is complete, payment to your PayID will continue to be directed to your Linked Account with us, unless your PayID is locked. If the other financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain with your current Linked Account. You can try to transfer your PayID again at any time.

- Transferring your PayID from another financial institution to Volt

To transfer a PayID from an account held with another financial institution to us will require you to start the process with that other financial institution and then complete the transfer with us by creating a PayID when you log in to your account.

- Maintaining and altering your PayID

You must keep your PayID details current, accurate and complete. Please notify us promptly of any change to your PayID details.

If you no longer own or have authority to use your PayID you must arrange to close your PayID immediately.

- Locking your PayID

We can lock your PayID at any time without notice if we reasonably suspect that your PayID has been used for a fraudulent purpose or there is suspected suspicious activity

relating to the use of the PayID.

You will not be able to transfer your PayID or receive payments addressed to your PayID while your PayID is locked.

- Closing a PayID

You can close your PayID at any time through the 'PayID' function in the Volt app or when you log into your account.

In closing a PayID, you confirm that:

- you are authorised to operate the account to which the PayID relates; and
- you have, or had in the past, authority to use, the PayID.

Closing a PayID will result in us removing your PayID from the PayID Service.

We can close your PayID where:

- we reasonably suspect that the PayID is or has been used for a fraudulent purpose;
- there is suspected suspicious activity relating to the use of the PayID;
- your PayID has remained locked for a period that we consider to be unreasonable; or
- we are required to do so by law or by the operator of the New Payments Platform.

We will automatically close your PayID:

- if the Linked Account for that PayID is closed (unless you are working with us to open another account);
- where there is evidence that you no longer have the right to use it or it is no longer in use;
- if it has not been used in 3 years; or
- if it has been inactive for 3 months or more and we have been unable to contact you to resolve a conflict with someone else using or attempting to use the same PayID.

- Receiving money to your PayID

Not all accounts and payment types support payment to a PayID. The ability for a payer to pay your PayID depends on the payer's financial institution and on the type of account and payment to be made. As a result, in some cases you may need to provide your BSB and account number to the payer to arrange a payment.

- Mistaken and Misdirected Payments

Where an NPP Payment made to your account is made by mistake, we may, without your consent, deduct from your account an amount equal to that mistaken payment. A payment made by mistake includes a fraudulent payment, an over payment, a duplicate payment, a payment error made by us or a Misdirected Payment.

- Making Payments to a PayID

Not all accounts have PayID but you do not need to have PayID in order to make a payment to someone.

If you do not give us all of the information required by Volt to make a payment or if any of the information you give us is inaccurate we may not be able to make the payment.

When you enter the PayID in the payee field of the relevant service, we will check to confirm that the PayID has been created in the PayID Service. Where it has, we will display to you on screen the Shortname attached to that PayID. You must check that the Shortname displayed matches the person that you intend to pay. If you do not recognise the Shortname or the Shortname does not match who you intend to pay, you should contact your intended payee to confirm that all details are correct before proceeding to make the payment. Incorrect details could result in a payment to the wrong account and may result in loss of your funds.

Once an NPP Payment is made we will not be able to cancel it so it is important that you confirm the information you provide to us is correct.

Where you make a NPP Payment from an account that has a debit card attached to it, you are making the payment from the account and not the card and as such chargeback rights do not apply.

When you direct a payment to a PayID connected to a joint account, the other accountholders may be able to see the messages and notifications associated with the payment.

- How we process future dated payments to a PayID

Volt will soon be introducing the ability to make future dated payments to a PayID. We will let you know once this functionality is enabled.

Once future dated payments are available we will attempt to make payments on the nominate scheduled payment dates. As a result you should ensure that you have sufficient funds available in your account to make the payment. We may decline to process the payment if, at the time we try to make the payment, you don't have sufficient funds in your account.

On the scheduled payment day, before we try to make the payment we check the PayID Service to confirm whether the PayID and/or BSB and account is still registered and whether there has been a change in the name attached to the PayID since the time you set the payment up. We won't be able to process the payment if the PayID is no longer registered or is locked, and we won't process the payment if the name attached to the PayID has changed. You should check the payment status at the end of the day that the payment was scheduled to be made to confirm whether it has gone through.

- Suspension and termination

You may stop using the PayID Service at any time.

PayID may also be temporarily unavailable to enable us to make system maintenance or upgrades.

If our participation in, or the provision of, the New Payments Platform is suspended, ceases or cancelled at any time we will be required to terminate the PayID Service. We will provide you with as much notice of this as is possible if this occurs.

Notification may include by posting to our website or through direct communication with you.

- OSKO

Volt will be subscribing in future to Osko under the BPAY® Scheme. We will let you know once this functionality is enabled.

All eligible accounts will be able to receive or send Osko Payments. You will need to use the Volt app in order to view full remittance details or other data that is sent with an Osko Payment to your account. When making an Osko Payment, you must not enter inappropriate payment descriptions such as insulting or defamatory text. We will not be liable to you or any other person for inappropriate payment descriptions.

- Payments using Osko are not BPAY payments

For eligible accounts, you can make Osko Payments through our Volt app or other login. We will not be obliged to make an Osko Payment if you do not give us all of the information we require or if any of the information you give us is inaccurate.

You can make Osko Payments to a PayID or to a BSB and account number, provided that the account that you are paying is able to receive Osko Payments. Some payees might not be able to receive Osko or NPP Payments, depending on their account or payment type or their financial institution.

If the PayID or account that you entered does not accept Osko Payments but is capable of accepting other types of NPP Payment, we may send the payment as another NPP Payment type. In this case, we will still send the payment in near real-time but the timing of making the funds available to the payee is at the discretion of the receiving bank.

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

Where you make an Osko Payment from an account that has a debit card attached to it, you are making the payment from the account and not the card and as such chargeback rights do not apply.

When you receive an Osko Payment it will immediately form part of the available balance of your account, even if you receive the Osko Payment after the end of a banking day. However, where you receive an Osko Payment after the end of a banking day, that payment may not be included in the balance of your account for other purposes (such as interest, fees or overdrawing calculations) until the next banking day.

- Suspension and termination of OSKO

You may stop using the Osko service at any time.

NOTE: We may stop using OSKO or suspend OSKO or NPP payments from your account.

We may suspend your ability to make Osko Payments or other NPP Payments at any time where we believe on reasonable grounds that it is necessary to do so to prevent loss to Volt

or you, including where we suspect that the service is being used or will be used in a fraudulent manner.
We may also make the service temporarily unavailable for the purpose of performing system maintenance or upgrades.

We will be required to terminate the Osko service if our membership with BPAY or our participation in Osko is suspended, ceases or is cancelled or if BPAY ceases to provide the Osko service. We will provide you with as much notice of this as is possible in the circumstances if this occurs.

Notification of the above may include by posting to our website or through direct communication with you.

- Privacy and NPP and Osko

By registering your PayID, you agree to your registration with the PayID Service provided on behalf of Volt by Australian Settlements Limited and hosted by NPP Australia Limited.

In order to provide you with the NPP service and Osko service, we may need to disclose your Personal Information to third parties. You consent to the collection, storage, use and disclosure of information about you (such as your PayID, PayID Name and account details) for Volt and other parties to access, use, disclose and store when facilitating payments or registering and validating PayIDs, including NPP Australia Limited, BPay Pty Limited, Reserve Bank of Australia, Australian Settlements Limited, other PayID Service participants or financial institutions and service providers to these entities.

When making NPP payments or creating and amending a PayID via the Volt app, Volt monitors your transactions to track fraud. To do this we need to access, collect and store data about your device, such as its IP address and location at the time of making the NPP payment or creating and amending a PayID. To the extent that this data constitutes personal information, we will deal with it in accordance with our Privacy Policy available at: voltbank.com.au/privacy-policy.html

To help payers identify who they are paying, your PayID Name may be displayed alongside your PayID to any person that enters your PayID as the address for an intended payment. For example, if your mobile number is your PayID, then any person who enters your mobile number in the payee address field of their internet banking may see your PayID Name attached to that mobile number.
Where you hold a joint account, other account holders may be able to see messages and notifications associated with payments and other messages addressed to your PayID.

If we are not able to access, collect, store, use and disclose your Personal Information as set out in this section, then we may not be able to provide you with the NPP or Osko services.

22. ▼ BATCH ENTRY PAYMENTS
(Corporate Cash Management Accounts only)

You may only make a batch entry payment where you're making a Pay Anyone payment on your own behalf; or on behalf of one or more of your related entities or principals to discharge debts.

In making a batch entry payment you warrant to us that when you make the batch entry payment that:
- the batch entry payment is validly authorised and that you have obtained a written direction from the principal or related entity (End Client) to make that batch entry payment
- you're making that batch entry payment on your own behalf; or on behalf of your related entities or principals to discharge debts
- the payments are not (or are not intended to be) part of a business of making BPAY payments on behalf of third parties, but rather, it is making payments as an incidental part of your ordinary business

If you make a Batch Payment you must:
- maintain a list of any End Client and provide that list to us upon request
- maintain systems and processes which allow payments and adjustments (including credits and reversals) in relation to those End Clients to be separately identified and differentiated
- promptly notify us if you become aware or reasonably suspect, any fraudulent or illegal activity involving payments to those End Clients

You will notify us in writing of any non-compliance by you with these terms and conditions in connection with making a batch entry payment promptly after becoming aware of the non-compliance.

Should you wish to make batch entry payments you consent to your personal information and that of your customers or principals, as well as such transactional information as is necessary to process your payments.
non-compliance.

Should you wish to make batch entry payments you consent to your personal information and that of your customers or principals, as well as such transactional information as is necessary to process your payments.

23. SYSTEM MALFUNCTION

You are not responsible for loss caused by a system or equipment, supplied by any party to a shared electronic network, failing to complete a transaction that system or equipment accepted on your instructions.

If you should have been aware that the system or equipment was not available or not working properly, we may limit our liability for losses under this term to:

- correcting any errors
- refunding any fees or charges you incur relating to the failure of that system or equipment

24. GENERAL SECURITY TIPS

Here are some general thoughts on keeping your Internet Banking life safe and secure.

We recommend that you:

- use virus protection software on all electronic devices you use for access to the internet;
- be wary of emails (phishing emails) that ask you for information about you or your bank accounts or that ask you to click through a link in the email. They can result in giving a fraudster access to your personal information or introducing malware into your computer.

Please note:

- we will never send an email asking for your username or passcode, or asking you to click on links in an email concerning these;
- it is your responsibility to make sure you have and pay for all necessary connections, like PC equipment and software, a secure telephone line, electricity and a secure internet service provider, to enable you to access our electronic banking services; and
- we will accept blame for failures by us but we are not responsible for services we cannot give you due to you not taking adequate security or anti-virus measures.

25. PRIVACY AND DATA COLLECTION

We are careful to protect the personal information we collect about you. We may use your personal information to help us manage our relationship with you efficiently and assist us to improve our service to you.

- Volt collection

Volt may collect personal information about you to enable your Volt account to properly function, for security purposes and for Volt to:

- better assist you, if you contact us for help;
- tell you about other products or services that may be of interest to you; and
- further develop your account.

Further information about how Volt uses data is available in our Privacy Policy available at: voltbank.com.au/privacy-policy.html.

- Third parties

Volt also uses a number of third parties to collect information about you for your security and to tell us how you use the Volt account. Generally, they do not collect personal information about you.

Volt uses the information third parties collect for us to:

- report system crashes;
- perform statistical analysis of aggregate user behaviour;
- give you assistance;
- further develop the Volt account;
- detect potentially fraudulent activity; and
- ensure the Volt account functions properly.

Volt will not use this information in any other manner. You agree that Volt and the third parties may collect and store various information about you for these reasons.

If you do not consent to the collection of this information you should cease using the Volt account.

26. COMMUNICATIONS

We communicate with you electronically to the email address you nominated in the application for your account and in any other way we are legally permitted, including advertisement and SMS. That communication includes notification around availability of account statements and changes to these terms and details of upcoming system maintenance. We expect there will be other communication.

We want to keep up with you. If you change your:

- email address
- mailing address
- residential address or
- phone number

please email us at customercare@voltbank.com.au or contact us by Live Chat in the Volt app or phoning us on 13 VOLT (13 8658) during our standard business hours.

We may ask for additional information before we make some changes for your own protection and to ensure we have the right details about you.

27. CHANGES TO THESE TERMS

NOTE: We may change any of these electronic banking terms.

We tell you about any changes to these terms in the same manner specified under Part E of your Volt Account Terms and Conditions. Most changes under these Electronic terms will take effect immediately or on the same day as you are notified.

- Transaction limit changes

If we change the terms to remove or increase a limit on a transaction, we tell you how the change may increase your liability for unauthorised transactions under clauses 14 and 15.

The current version of these terms will always be available to view at voltbank.com.au/electronicterms.html.

28. COMPLAINTS

From time to time, we may get it wrong. If this happens, please tell us. We appreciate constructive feedback. The more information you give us, the easier it will be for us to improve.

- Contact

Get in touch with our Customer Care team if you want to:

- find out the interest rates on your account
- understand terms that are not clear to you
- provide feedback on how we can improve our products or services
- make a complaint

Please email us at customercare@voltbank.com.au or contact us by Live Chat in the Volt app or phoning us on 13 VOLT (13 8658) during our standard business hours.

We'll do our best to answer your questions within one business day. It may take us a bit longer to deal with complaints if we have to investigate.

- Mistaken Pay Anyone payments

You can complain to us under this clause if you are unhappy with the way we deal with your report about a mistaken payment under clause9. We will deal with your complaint as set out in this clause.

- Unauthorised transactions

If you complain about a transaction you believe to be an unauthorised transaction, we will manage your complaint in accordance with the ePayments Code. We will ask you for certain information about:

- that transaction; and
- the way you looked after your username and passcode.

We will investigate your complaint as quickly as we can. In most cases, we expect to determine an outcome for your complaint within 45 days after receiving it. It will help us to resolve your complaint quickly, if you give us all the information we request quickly.

Within 21 days after receiving your complaint, we will give you a status report and tell you either:

- the outcome of our investigations; or
- that we need more time to investigate.

■ Taking it further

If you do not agree with the outcome of our investigations or if you consider we have not complied with the ePayments Code in managing your complaint, you can take your complaint to the Australian Financial Complaints Authority (AFCA), the external dispute resolution scheme of which we are a member.

AFCA is free to you. If you ask them to review your complaint, AFCA will discuss the complaint with you and us while they seek to resolve the complaint.

■ AFCA's contact details

Australian Financial Complaints Authority (AFCA)
9:00am–5:00pm AEST weekdays

TELEPHONE:
1800 931 678 (free call within Australia)EMAIL:
info@afca.org.au

MAIL:
Australian Financial Complaints Authority Limited GPO Box 3 Melbourne, VIC 3001

FAX:
(03) 9613 6399

If you have a complaint about the way we manage your personal information, you can make a complaint to AFCA or to the Office of the Australian Information Commissioner (OAIC).

■ OAIC contact details

EMAIL:
enquiries@oaic.gov.au

TELEPHONE:
1300 363 992

29. ▼ GOVERNING LAW

These terms are governed by the law of New South Wales. If any term is invalid or unenforceable for any reason, the particular term will be void and the remaining terms will continue to govern your use of our account.

30. ▼ WHERE TO GET HELP

If you:

- want us to explain any of these terms to you; or
- have read these terms and any FAQs and still cannot find the answer to questions; or
- just want to chat about ideas you have for improving our products or services

please email us at customercare@voltbank.com.au or contact us by Live Chat in the Volt app or phoning us on 13 VOLT (13 8658) during our standard business hours.

You can also visit the FAQ page on our website at voltbank.com.au/help.

■ Security concerns

You can report security breaches and unauthorised transactions by using the Volt app or by phoning us on 13 VOLT (13 8658). More details on this at clause 13.

31. ▼ PERSONAL FINANCE MANAGER TERMS (PFM)

■ What is the PFM service?

We give you access to an automated service (the PFM Service) you can use to manage your finances and assist you to achieve your financial goals. You can use it to collect information about accounts you hold with different financial institutions and to categorise what you spend money on.

Depending on whether or not you use a Partner App to open a Volt account and whether that Third Party Partner uses a PFM Supplier who uses Open Banking or Yodlee, you may need to disclose your usernames or passwords to the PFM Service Supplier to obtain the PFM Service if Yodlee is used. The PFM Service Supplier may then disclose your usernames and passwords to other service providers that assist it with the PFM Service.

NOTE: Your other financial institutions may not agree to you disclosing usernames and passwords to use the PFM Service.

Normally, the terms on which financial institutions issue usernames and passcodes to you require you to keep those usernames and passwords secret. You may breach those terms if you tell anyone else those usernames or passwords.

We do not want you to breach the terms you agreed with other financial institutions. Please contact them to check if they are OK with you disclosing the username and password they gave you so you can use the PFM Service, before you sign up for the PFM Service.

- Eligibility

We make the PFM Service available at no extra cost to you through the App.

- PFM Service terms

If you wish to use the PFM Service, the following terms will apply to that use. You agree to the following terms when you proceed to use the PFM Service.

- Using the PFM Service?

If you open an account directly with us we use Open Banking to provide you with the PFM Service. Open Banking is a secure way for you to share your banking data amongst accredited data recipients such as other financial institutions.

When you use the PFM Service, you can:

- authorise the PFM Service Provider and its Service Providers to act on your behalf to access certain information, like third party websites you nominate;
- ask the PFM Service Provider or its Service Providers to register accounts you hold and from which you request the PFM Service Provider or its Service Providers to collect your financial information for you;
- direct the PFM Service Provider to:
  - receive Account Information about accounts held in your name, or jointly by you and another or others, maintained online by other institutions of which you are a customer; and
  - maintain accounts you hold or engage in financial transactions on your behalf.

The PFM Service Provider may work with one or more online services to access Account Information.

The PFM Service Provider manages your personal information in accordance with privacy notices we give you and the PFM Service Provider's privacy policy available at https://frollo.com.au/privacy-policy.

- Account Information

When you use the PFM Service, you will be asked to give information about yourself and Account Information. So that the best service can be given to you, please ensure that Account Information is accurate, up to date and complete whenever you use the PFM Service.

You must not misrepresent your identity or Account Information. Otherwise, the PFM Service Provider may suspend or cancel your use of the PFM Service.

- PFM Service notices

We and the PFM Service Provider will send notices about the PFM Service electronically to the email address we use to contact you about your account.

Use of the PFM Service is personal to you. You cannot assign use of the PFM Service to another person.

You may use the PFM Service only for the purpose for which it is made available to you. You must not use the PFM Service for unlawful purposes or in any way that may damage the reputation of the PFM Service, the PFM Service Provider or us.

You must not copy, download, reproduce or distribute any information contained in the PFM Service without the PFM Service Provider's prior written consent.

- Seeking professional advice – expert advice

The PFM Service Provider does not hold an Australian Financial Services Licence and cannot give you financial advice. So, for example, the PFM Service Provider cannot tell you whether one account you hold is better than another or whether you should open a particular account.

The PFM Service assists you to manage your finances. Any information you get from the PFM Service is general information only and does not consider your individual circumstances, objectives, financial situation or needs. It does not give you financial, legal, tax or product advice or take the place of professional advice.

Please seek professional advice, if you wish to make investment decisions or buy financial products relying on any information you get from the PFM Service.

- PFM Service problems

We cannot, and the PFM Service Provider may not be able to, control technical or other difficulties that result in:

- interruptions to the PFM Service;
- failures to obtain your data;
- subject to our obligations under Privacy law, loss of data that the PFM Service Provider collects on your behalf through the PFM Service; or
- loss of personalized settings you put in place on your accounts.

There may be times at which the PFM Service Provider suspends the PFM Service generally to maintain or to protect the security of PFM Service users or the security of the PFM Service itself. It may not be possible to tell you in advance of that suspension, but we will work with the PFM Service Provider to overcome the cause of it as soon as possible.

- Cancelling the PFM service

You may cancel your access to the PFM Service at any time through the app. You cannot cancel your access to the PFM Service merely by deleting the PFM Service app from your device.

The PFM Service Provider may cancel or suspend your access to the PFM Service at any time if you breach an important condition in the PFM Service Terms. We will seek to give you advance notice of any proposal to cancel or suspend your access to the PFM Service, unless the PFM Service Provider needs to cancel or suspend your access urgently to protect the security of PFM Service users or the PFM Service itself. The PFM Service Provider may retain de-identified information it collects about you and aggregate that information with other de-identified information it holds to assist it to improve the PFM Service.

32. ▼ DEFINITIONS

ACCOUNT means any account you have with Volt which you can only access by way of Electronic Banking.

ACCOUNT INFORMATION refers to any information you provide under clause 31 in relation to accounts you hold with other financial institutions.

APPLE® means Apple Inc. and is a trademark of Apple Inc., registered in the U.S. and other countries.

APPLE PAY means the service provided by Apple that enables you to make Apple Pay Payments. Apple and Apple Pay are trademarks of Apple Inc., registered in the U.S. and other countries.

APPLE PAY PAYMENT means a contactless transaction used by holding your Device to a contactless terminal until the transaction is completed. This includes merchant mobile sites, mobile applications and websites which permit you to use Apple Pay to make your payment and any other method allowed by Apple from time to time. This also includes refunds processed using Apple Pay.

APPLE PAY TRANSACTION RECEIPT means a receipt which complies with the ePayments Code and provides you with details about your transaction including the Device used for the transaction.

ASIC means the Australian Securities and Investment Commission.

ATM means automated teller machine that accepts plastic cards for cash withdrawals and other account services.
BILLER is any person you can make a payment to using BPAY®.

BATCH ENTRY PAYMENT means the method of making Pay Anyone payments to one or more recipients by you compiling and submitting an electronic file to us containing one or more payer directions.

BPAY® is a registered trademark owned by BPAY Limited ABN 69 079 137 518 and a system you can use to make payments from your Volt Spend or CMA account to others, generally, suppliers of goods or services to you.

BPAY® SCHEME means the scheme operated by BPAY which governs the way in which Osko is provided.

BUSINESS refers to an individual who is a sole trader operating a "small business" which means at the time of opening an account all of the following apply:

(a) the individual had an annual turnover of less than $10 million in the previous financial year; and
(b) the individual has fewer than 100 full-time equivalent

employees; and
(c) the individual has less than $3 million total debt to all credit providers including:
(i) any undrawn amounts under existing loans;
(ii) any loan being applied for; and
(iii) the debt of all its related entities that are businesses.

CASH MANAGEMENT ACCOUNT or CMA refers to an account that is available to for personal, individual business, Self-Managed Super Funds and corporate customers.

DEBIT CARD means a Volt debit Mastercard® we will issue to you which allows you to transfer money electronically from your Volt Spend account when making a withdrawal or purchase.

DEVICE means a device such as a phone, tablet or smartwatch which contains near field communication (known as NFC) technology and uses an operating system on which we determine, in our sole discretion, Volt debit cards may be registered.

DEVICE ACCOUNT NUMBER/ VIRTUAL ACCOUNT NUMBER means the number created by Mastercard® and Apple or Google (as applicable) and stored on your Device for use when making an Apple Pay or Google Pay Payment. This number is unique to your Debit Card stored on your Device and represents your Debit Card number for transactions using Apple Pay or Google Pay (as applicable).

DIRECT ENTRY means internet banking transactions to and from Volt accounts through use of direct debit and direct credit instructions.

EPAYMENTS CODE means the set of rules we subscribe to for the way we manage electronic transactions. All transactions you can make on your account are electronic transactions. The ePayments Code is set out in more detail in the Volt Electronic Banking Terms and Conditions.

GOOGLE® means Google Asia Pacific Pte. Ltd ABN 54 341 015 381 and/or its related bodies corporate and affiliates.

GOOGLE PAY means the service provided by Google that enables you to make Google Pay Payments

GOOGLE PAY APP means the app called by that name available from the Google Play store which you will find on your Device.

GOOGLE PAY PAYMENT means a contactless transaction used by holding your Device to a contactless terminal until the transaction is completed. This includes merchant mobile sites, mobile applications and websites which permit you to use Google Pay to make your payment and any other method allowed by Google from time to time. This also includes refunds processed using Google Pay.

GOOGLE PAY TRANSACTION RECEIPT means a receipt which complies with the ePayments Code and provides you with details about your transaction including the Device used for the transaction.

LINKED ACCOUNT' means an account linked to a PayID.

MASTERCARD® means Mastercard International Incorporated. Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated.

MASTERCARD RULES are the rules Mastercard issue from time to time which we and merchants are obliged to follow.

MISDIRECTED PAYMENT means a NPP Payment erroneously credited to the wrong account because of an error in relation to the recording of the PayID or

MONTH is a calendar month.

NPP® means the New Payments Platform operated by NPP Australia Limited.

NPP PAYMENT means a faster payment cleared and settled via the NPP in near real-time and includes Osko Payments.

OSKO® means the Osko Payment service provided by BPAY Pty Ltd.

OSKO PAYMENT means a payment which can be made in only seconds to another payee using Osko. Osko Payments are unique in that the industry is committed to processing 95% of these payments into recipient accounts within 15 seconds, and 99% of transactions into accounts within one minute.

PASSCODE is any password or code that you create or that

we or any third party gives you that must be used before we or the third party processes a transaction. This includes PINs, internet, phone, mobile banking, passwords and codes generated using a security token.

PAY ANYONE is a way to transfer funds, between accounts you hold in Australia, using the Direct Entry system.

PAYID means a unique identifier and which is any of the following, which can be linked to an account for the purpose of directing a NPP Payment or instructions to that account:

- a telephone number or email address; or
- any other type of identifier as permitted by NPP and supported by us.

PAYID NAME means the name registered with a PayID which identifies the owner of the account associated with the PayID Service.

PAYID SERVICE means the payment addressing service for sending and receiving a NPP Payment.

PARTNER APP means the app or other online banking access of a Third Party Partner used to access a Volt Account.

PERSONAL INFORMATION is information or an opinion about you, as an individual, and from which you can be identified.

PFM SERVICE is the Personal Finance Manager (PFM) account aggregation and transaction categorising service we make available under clause 31 of these terms.

PFM SERVICE SUPPLIER means Frollo Australia Pty Ltd or such other supplier we may decide to use from time to time to provider the PFM Service.

"PIN" means a personal identification number which is a numerical code that may be required to be entered as an additional security layer to complete various financial transactions.

SINGLE CREDIT TRANSFER or SCTs means a credit payment message, other than an Osko® payment, which allows for single payments to be sent and received by NPP within a few hours for the benefit of a payee with another NPP participant.

SMS stands for Short Message Service and is the most widely used type of text messaging to your mobile phone.

STANDARD BUSINESS HOURS 8.00am – 8.00pm (Sydney time), five days a week (excluding Australian public holidays and NSW state based holidays).

THIRD PARTY PARTNER means any third party you use to apply for an account with Volt.

TWO-FACTOR AUTHENTICATION is when we send a code to you, in order to confirm certain requests or transactions relating to your account.

USERNAME is the email address that you can use with your passcode for accessing your account via the Volt app.

VOLT ACCOUNT means, as applicable, your Volt Spend, Volt Save or Volt CMA account.

VOLT APP means an app for compatible iOS and Android mobile phones and/or tablet devices to enable you to open and operate your account.

WE, US and VOLT means Volt Bank Limited ACN 622 375 722 Australian Financial Services Licence 504782 and our means belonging to us.

YODLEE means Yodlee Inc, a US company which supplies a PFM Service through use of your usernames and passwords to access information about accounts you hold at other financial institutions.

YOU is a person that applies to open or opens an account with us.

ACN 622 375 722 Australian Financial Services Licence and Australian Credit Licence 504782