



**ELECTRONIC
BANKING
SAVE & SPEND
TERMS & CONDITIONS**

Effective 1 May 2020

■ CONTENTS

1. ePayments Code	1
2. What is an unauthorised transaction?	1
3. Accessing information and functionality	1
4. Volt Spend	1
5. Mastercard® Debit Card	2
6. Deposits	4
7. Withdrawals and payments	4
8. Stopping transactions	4
9. Mistaken payments direct entry ('Pay Anyone') facility	4
10. Balances and transaction records	6
11. Fees and charges	6
12. Security requirements	6
13. Reporting security breaches and unauthorised transactions	7
14. When you're not responsible for unauthorised transactions	7
15. When you're responsible for unauthorised transactions	7
16. When you contribute to losses from unauthorised transactions	8
17. Limit on your liability for unauthorised transactions	8
18. Shared network	8
19. System malfunction	8
20. General security tips	8
21. Privacy and Data Collection	8
22. Communications	9
23. Changes to these terms	9
24. Complaints	9
25. Governing law	10
26. Where to get help	10
27. Definitions	10

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 27.

▼ 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

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.

■ Volt app

With a Volt Save or Volt Spend Account you can use your Volt app 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);
- 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
- view your transaction history.

A daily transaction limit of \$20,000 applies to Pay Anyone transactions.

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

Sometimes, the Volt app will not be available. That could be due to routine maintenance on the app 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. We may not be able to give you notice of emergency maintenance.

▼ 4. VOLT SPEND

Clauses 4 and 5 apply only to Volt Spend

■ 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 from your account.

With a Volt Spend account, you can also make Direct Entry payments and direct debits and transfers between accounts in your name.

■ BPAY®

By using BPAY you can make payments or transfer money from your Volt Spend account. 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 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.

▼ **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.

■ Locking or Cancelling your Debit Card

Contact Customer Care using live chat within the Volt app if you would like to lock or cancel your debit card. If your debit card is locked, you won't be able to use it to make purchases or withdraw from an ATM.

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.

■ 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 in 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

You can deposit money into your account through Pay Anyone from another account held with another financial institution. 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. These limits may apply to your opening and ongoing balance.

▼ 7. WITHDRAWALS AND PAYMENTS

To withdraw or make payments from your account you will need to use the Pay Anyone facility to transfer money to another account held in Australia. You will need the BSB and number of the account to which you wish to make the transfer or payment. Scheduled and recurring payments are not available at this time.

Please take care when you enter the details of the other account. The Volt app will warn you to check the payment details you entered before you complete a Pay Anyone 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
- 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 cooperate 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 can 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 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 downloading, installing and registering for the Volt app. You may have to pay fees and charges on transactions you make using the Volt app or 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 downloading, updating and using the Volt app. 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.

Generally, Volt does not allow other people to operate on

your account. If another person has stored their biometric information on your device in breach of these terms, you acknowledge that the person will be able to access your accounts including to view and conduct certain transactions on your account using the Volt app on your device. We will treat those transactions as having been authorised by you and conducted with your knowledge and consent.

Please take steps to ensure your mobile device is secure. Also, it is important to ensure that any biometric information used in connection with your mobile 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. 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.

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

Please choose passcodes that 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, we may block access to your account or you may be responsible for unauthorised transactions by use of that passcode on your account.

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

It is a good idea to change your passcode occasionally. You can change your passcode through the Volt app.

■ 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 app passcode". There are other examples.

Please make a good effort to keep your passcode secure.

■ Personal use only

You cannot authorise someone else to transact on your account.

Your passcode is for your use only. 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, the identity of your passcode 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

▼ **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 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 a passcode is no longer secure

▼ **15. WHEN YOU'RE RESPONSIBLE FOR UNAUTHORISED TRANSACTIONS**

■ 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 12, 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 13 or clause 14,

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. 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

▼ 20. 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.

▼ 21. 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 the Volt app 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 the Volt app.

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 app. Generally, they do not collect personal information about you. We will tell you if they do.

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 app;
- detect potentially fraudulent activity; and
- ensure the Volt app 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 app.

▼ 22. 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.

▼ 23. CHANGES TO THESE TERMS

We tell you about any changes to these terms in the same manner specified under Part E of your Volt Save or Spend 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

▼ 24. 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 clause 9. 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

▼ 25. GOVERNING LAW

These terms are governed by the law of New South Wales.

▼ 26. WHERE TO GET HELP

If you:

- want us to explain any of these terms to you; or
- have read these terms and 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.

▼ 27. DEFINITIONS

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

ANDROID DEVICE means a device such as a phone, tablet or smartwatch which uses the Android operating system, and

on which we determine, in our sole discretion, Volt debit cards may be registered.

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.

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

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

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.

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

MONTH is a calendar month.

PASSCODE is the code you create and that you can use with your username for access to the Volt app.

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

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

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).

TWO-FACTOR AUTHENTICATION is when we send a code to the Volt app, 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 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.

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



ELECTRONIC BANKING TERMS & CONDITIONS ▼ VOLT-002 (05/20)

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

© 2020 Volt Bank Limited (Volt Bank)