

Origin MMS Internet Access services terms and conditions

Section 1 – Overview of these terms and conditions

1. Overview

This document sets out the terms and conditions (**terms and conditions**) for *Origin MMS* online, mobile and tablet *Internet Access* services. *Internet Access* is a service that lets you check information about your accounts and tell us to perform transactions using those accounts. These terms and conditions are separate from and do not affect the terms and conditions applicable to any loan account or other account that you access via *Internet Access*.

The information in this document is subject to change. We may vary these terms and conditions and when we do we will post the current version on our website. Please check our website for the current version of these terms and conditions.

If you have any questions, please ask us

If there is anything in this document that you want to ask us about, simply contact us by:

- Calling us on 1300 767 063;
- visiting our website <http://www.originmms.com.au/contact-us>;
- writing to us at [PO Box A1244, Sydney South NSW 1235].

To report suspected unauthorised access or a security breach to your *Internet Access* please call our contact centre on 1300 767 063
8am - 7pm Monday to Friday (AEST)
8am - 5pm Saturday (AEST).

Our *Internet Access* offers you the convenience of conducting most of your electronic transactions at a time that suits you. You can access funds and transfer funds between your accounts, pay bills and make purchases 24 hours a day, 7 days a week.¹

When you make a transaction through your *Internet Access* you authorise us to act on the instructions entered into your *Internet Access* portal. Your electronic transactions are governed by these terms and conditions as well as the terms and conditions of your accounts, products and/or services being used. These terms and conditions reflect the *ePayments Code* which we have adopted and to the extent applicable we will comply with the *ePayments Code*.

Section 2 – *Internet Access* terms and conditions

2. Contractual relationship

These terms and conditions and the terms and conditions of your accounts, products and/or services being used, form the terms and conditions of the contract between you and us if you decide to open and use our *Internet Access*. These terms and conditions become binding once we give *Internet Access* and you accept and use such access method. As from that time, we and you undertake to be obligated by these terms and conditions. These terms and conditions apply to any instructions and information you give to us through *Internet Access*.

There are also further terms and conditions which may apply by operation of law, to any account you decide to open with us. It is not possible to set out in these terms and

¹ Regular system upgrades may limit access to your accounts through some services.

conditions all of the legislative, common law or other code provisions which may apply to a credit or account service provided to you. Please read these terms and conditions before using our *Internet Access*. You will then know what to expect from us and what we expect from you.

You can ask us questions about any of the terms and conditions you do not understand. If you use our *Internet Access* then you should keep a copy of these terms and conditions and all other documentation for future reference.

Definitions of important words and terms can be found in section 45 of this document..

3. User Set-up

To sign-in to *Internet Access* for the first time, you will need a *Customer Number* and a *Password*.

When you sign into your *Internet Access* for the first time, you'll be required to change the *Password* we provide to you. For your security, we recommend that you choose a *Password* for your *Internet Access* that is unrelated to any of your other *Origin MMS* passwords, such as your *Debit Card* PIN.

When you sign into *Internet Access* for the first time you'll also be required to:

- (a) confirm some personal information (including your email address and mobile number) to enable your use of *Internet Access* and *Origin MMS* protect SMS Codes.
- (b) for individual customers, agree to receive notices, documents and communications for your current and future accounts electronically through *Internet Access* and be notified to your email address when a document is

available to retrieve it (see sections 18 and 19 of this document).

- (c) We will handle your personal information as set out in the Privacy sections 36 to 39 (inclusive) in this document.

4. Notifications on your Mobile device

You need to enable notification on your mobile device for mobile *Internet Access* so we can send you notifications to your registered mobile device. Your mobile notifications can be enabled and disabled at any time by you via your settings on your mobile device.

Remember that anyone who has access to your mobile device will be able to see your notifications.

Some notifications are "*actionable*". This means that when you receive a notification, you can select it in order to access more information or perform an instruction.

Communications network or system outages, or other factors beyond our control (such as your internet connection or mobile device limitations) may delay or affect delivery and receipt of your mobile notifications. You may not be able to receive notifications if you have uninstalled your mobile *Internet Access* application on your device, or if your device has been deregistered.

We may without notice to you, temporarily suspend or terminate our notifications service for any reason.

5. Joint Accounts

Origin MMS may share a joint account within *Internet Access* once all account holders have signed up for *Internet Access*.

The operation of the account can be operated by either account holder in *Internet Access* for

all payments and transactions. Each account holder authorises us to process payments from a joint account created via *Internet Access*.

6. What are the risks?

There may be a risk that you may not be able to access your account information or make transactions through a service which is reliant on computer and/or telecommunications systems.

Origin MMS is dependent on the reliability of its own operational processes and those of its technology and telecommunications partners in respect of computers, computer networks and telecommunications.

Disruptions to these processes may result in your *Internet Access* services being unavailable from time to time.

7. Special risks relating to your *Internet Access*

While your *Internet Access* allows you to transact simply using your electronic equipment and codes, because of that simplicity, it also poses special risks such as the ones outlined below.

- (a) If someone else has your codes, they can transact on your account as if they were you. You may be liable for such transactions (refer to sections 26 and 34 of this document) for further details.
- (b) You should take special care to keep your codes secret and to not disclose them to any third-party including family, friends and institutions.
- (c) You should ignore any emails that appear to come from us that require you to input your codes. We will never send you such email requests. These emails may come from third parties

seeking to use the information to access your accounts.

- (d) You should also be careful about using services which offer to interface with our *Internet Access* services or other means of electronic banking on your behalf. For example, you may be led to believe that you are inputting your codes into our *Internet Access* services, while in fact you are disclosing your codes to a third party hosting a hoax website or mobile/tablet device application.

We continually look at ways to minimise any unauthorised transactions on your account. We may use various techniques from time to time, including contacting you after an unusual transaction or series of transactions to confirm that you did in fact authorise the transaction(s). Your access to our *Internet Access* and other means of undertaking electronic transactions may be suspended if we detect or suspect unusual activity which may be the result of malware or a computer virus, ID takeover, phishing or fraud. We reserve the right to withhold access to *Internet Access* where we continue to detect malware or a computer virus, or you refuse to follow our contact centre's recommendations provided to you to assist with the removal of malware and/or computer viruses from your computer, mobile or tablet device.

8. Legal Risk

As Australia is a member state of the United Nations, we are obliged to implement United Nations Security Council sanctions. Consequently, *Origin MMS* may be prohibited from dealing with certain persons or entities. This means that if we become aware that you are a *Prohibited Person* or entity, then we may be required to suspend, cancel or refuse you services or close or terminate any arrangement with you. We may also be required to freeze assets of yours. You could

incur significant costs as a result of these actions.

9. Refusal of service

(a) Despite any right contained in these terms and conditions, in the event that you or your joint account holder appears to be a *Prohibited Person*, then we may immediately:

- (i) refuse to process or complete any transaction or dealing of yours;
- (ii) suspend the provision of a product or service to you;
- (iii) refuse to allow or to facilitate any of your assets held by us to be used or dealt with;
- (iv) refuse to make any asset available to you to any other *Prohibited Person* or entity; or
- (v) terminate these arrangements with you.

(b) To manage our compliance with international laws and our financial and regulatory risk, we can also suspend or terminate the provision of a product and service to you while you are within sanctioned countries.

(c) We can also cancel any access method, including your *Debit Card*, PIN, *Password* or not process a transaction without notice if:

- (i) we think your account is being used unlawfully including fraudulently or in a way that might cause you or us to lose money; or
- (ii) we consider to do so is reasonably necessary, for

example, to comply with laws in Australia or overseas, card scheme rules, manage regulatory risk or if your instructions are not clear.

(d) We will be under no liability to you if we do any or all of these things.

(e) We may also at our discretion suspend or terminate the provision of a product or service to you (for example this may include suspending your *Internet Access*). When we do this, to the extent that we legally can, we will act fairly and reasonably towards you in a consistent and ethical manner. In doing so we will consider your conduct, our conduct and the accounts, products and/or services which are being used.

(f) If we exercise our rights under this section, you must pay any losses, costs or expenses that we incur in relation to any action taken under this section, including interest adjustments and/or administrative costs under these terms and conditions.

Section 2: Terms and Conditions

10. *Debit Cards, PINs and Passwords*

Debit Cards, PINs and *Passwords* remain the property of *Origin MMS*. To use your account, you must first sign your *Debit Card* and then activate it online as specified in the letter enclosing your *Debit Card*. Once activated your *Debit Card* can be used and is only valid only for the period indicated on it. You cannot use the *Debit Card* after the expiry month indicated on the *Debit Card*.

11. **How do you cancel or stop a *Debit Card*?**

You must tell us if you wish to cancel a *Debit Card* issued to you and also ask us to place a stop on your account, in which case you will

not be able to make any further transactions on the account until you ask us to remove the stop. Cancellation of a *Debit Card* or a stop may not take full effect immediately. You must follow the cancellation requirements set out in the *Conditions of Use Visa Debit* document provided to you.

You will continue to be liable for any transaction amounts not yet processed on your *Debit Card* and for all transactions made using a *Debit Card* at a time when any of our electronic transaction systems are unavailable, until you have taken all reasonable steps to have the *Debit Card* returned to us and cancelled in accordance with the requirements set out in the *Conditions of Use Visa Debit* document.

You will also be liable for *Debit Card* transactions to purchase goods and services at a price below a merchant's authorised floor limit or where no authorisation is required, until you have taken all reasonable steps to have the *Debit Card* destroyed or returned to us. You authorise us to debit any outstanding *Debit Card* transaction amounts on your accounts to any other Account in your name.

12. Checking your transactions

Make sure you keep all receipts and transaction records you receive from merchants and check them against the transactions on your statement. Offline transactions processed by a merchant (including some contactless transactions) may not appear on your statement with the same date as the date you made the transaction. It is your responsibility to ensure there are sufficient funds in the account when this transaction is processed by *Origin MMS*. If you have access to your *Internet Access*, you can check the transactions online.

Where *Debit Card* purchases or transactions are made overseas (such as purchases made over the internet), they may be processed

using the date overseas (value date), which may not be the same as the date in Australia. This means that it may be processed using the balance in your account on that value date (as shown in your statement).

13. Authorising your transactions

Some merchants, e.g. restaurants, hotels and car rental agents, may ask us to confirm that your account has sufficient available balance to meet the estimated cost of the goods and services. We treat this as a request for authorisation.

We may choose not to authorise a particular transaction. For example, there may be security issues with the transaction or network or, you may have insufficient funds in your account.

If we do authorise a transaction, we reduce your available account balance by the estimated cost of the goods and services. Normally, this is then cancelled out when the actual transaction is completed.

However, in the following situations, your available account balance may be reduced for up to six *Business Days* after the authorisation date:

- (a) the merchant did not complete the transaction (e.g. you decided not to purchase the goods or services); or
- (b) the actual amount the merchant charged to your account was different to the original amount we authorised and the merchant didn't cancel the original authorisation (e.g. a hotel might get authorisation for one night's accommodation when you check in but the amount later processed to your *Debit Card* might be different to that authorisation.

14. Recurring transactions

You may authorise a merchant to regularly charge amounts to your account. To cancel the authority, you can cancel at any time either by informing *Origin MMS* directly or contacting and cancelling through the merchant. You should cancel at least 2 *Business Days* prior to any direct debit payment due as the payment may still go through until the cancellation is processed. Cancelling your direct debit does not cancel your contract with the merchant. If you still have a valid contract with a merchant and you've cancelled a direct debit, you'll need to make alternate payment arrangements with them. Or if you no longer require their services, you'll have to cancel your agreement with them where possible.

15. Refunds

A merchant must issue a valid credit voucher to make a refund to you. We can only credit the refund to your account when we receive the credit voucher from the merchant's bank.

16. Requesting a chargeback

In some cases, Visa's scheme rules allow us to dispute a transaction and request a refund of the transaction (i.e. chargeback) for a disputed transaction. The process of requesting a chargeback is set out in the *Conditions of Use Visa Debit* document provided to you.

17. When we may block a transaction

You may only use your *Debit Card* for lawful purposes. We may block purchases from certain websites or merchants if we have reason to believe that the products or services being offered:

- (a) are illegal (under Australian law or the laws of other countries);
- (b) contain offensive material; or

- (c) pose a risk to either systems or the integrity of transactions or information.

18. Sending you electronic communications

We provide statements and notices electronically where:

- (a) you have selected an account or service which only offers statements and notices electronically; or
- (b) the terms and conditions for that account or service permit us to do so.

Where applicable, we will give you your statements and notices electronically through:

- (a) Your *Internet Access* (or in the case of notices, we may post the notice on our *Origin MMS* website) – We'll let you know when the information is there by:
 - (i) email to an email address you have given us for contacting you;
 - (ii) SMS message to a mobile telephone number you have given us for contacting you; or
 - (iii) push notification from the *Origin MMS* App that the information is available for retrieval by you; or
- (b) any other means we agree with you or notify you that we will use to communicate with you.

You can change your electronic address on your *Internet Access* or by calling us on 1300 767 063.

We record that you received an electronic statement or notice on the day that we send our notification to your email address.

For changes to these terms and conditions, we notify these only by electronic delivery

(using any of the methods set out above) and paper copies are not provided.

Even if we normally provide electronic notices or statements, we reserve the right to send paper ones instead to your nominated postal address (e.g. if for any reason we are not able to provide them electronically or we cancel your election to receive statements or notices electronically because we are unable to deliver emails to your nominated email address).

As part of our *Internet Access*, we may from time to time send you messages, e.g. to your *Internet Access* inbox, including commercial electronic messages advertising, promoting or offering new or existing products or services.

You agree to receive such messages and that commercial electronic messages need not contain information about how to unsubscribe. We will however honour any preferences you make generally as to the receipt of marketing materials and your preferences in your *Internet Access* concerning product upgrades and new product offers.

19. Receiving your electronic communications and agreements

(a) You are responsible for the acts and omissions of all users, including any person you authorise to act for you. Except for electronic transactions, all communications and acceptances, including electronically signed documents, received by us from any person logged into your *Internet Access* using your *Customer Number* and *Password* are deemed to be authorised by you unless you can prove that you did not authorise the person and that:

- (i) without your knowledge your electronic equipment has been taken over by use of malware despite you having up to date

antivirus, antimalware and firewall software installed on your electronic equipment; or

- (ii) the person gained access to your *Customer Number* and *Password* without your approval despite you taking all reasonable precautions to prevent such access; and
- (iii) you did not unreasonably delay in reporting to us the compromise of your electronic equipment or the loss, theft or misuse of your *Customer Number* and *Password*.

- (b) If you agree to enter into agreements electronically or to electronically sign documents, you must do everything you can reasonably do to protect your *Customer Number* and *Password* from becoming known to any other person including by installing and maintaining up to date antivirus, antimalware and firewall software on your electronic equipment.
- (c) You must not disclose your *Password* to any other person.
- (d) You must not keep a record of your *Customer Number* and *Password* without making any reasonable attempt to protect the security of the record, such as making a reasonable attempt to disguise the *Password* within another record, hiding the record where it would not be expected to be found or keeping the record in a securely locked container or in *Password* protected device.
- (e) You must not choose a *Password* that represents your date of birth or name.

20. Entering the correct information in electronic transactions

When you make a transaction with electronic equipment, it is your responsibility to tell us the correct amount you wish to pay or transfer, and the correct account to which you wish to have the payment or transfer credited. The account name of the recipient does not form part of your payment instructions and will not be used or checked by us in making your payment. If you tell us to make a payment or transfer and after we have implemented your instructions, you discover that:

- (a) The amount you told us to pay or transfer was greater than the required amount, then you have to seek a refund from the recipient, and you cannot make a claim on us.
- (b) The account you told us to make a payment or transfer to was incorrect, you can contact the recipient to obtain a refund or contact us.² In addition, your terms of conditions of your account outline how mistaken payments are handled and recovered.

² *We will attempt to recover the funds on your behalf but we are not liable unless we fail to comply with the process and timeframes set out below. We will acknowledge receipt of your report and provide you with a reference number which you can use to verify that your report has been recorded by us and to enquire about progress of your claim. Once we have the information we require and are satisfied that you have made a payment to an unintended recipient, we will send a request for return of the funds to the unintended recipient's financial institution. Where your report is made within 10 Business Days of the mistaken payment and the unintended recipient has sufficient credit funds in their account, we may be able to take advantage of industry rules which allow us to recover the funds for you without the unintended recipient's consent.*

21. Contactless payments

For contactless payments, per payment limits apply as set by the relevant Visa *Debit Card* scheme.

22. Daily withdrawal limit

The daily *Debit Card* withdrawal limit is the total amount that can be withdrawn using a PIN from all accounts linked to a *Debit Card* in any one day. You can confirm and/or change your daily *Debit Card* withdrawal limit at any time by contacting us. If you request a higher daily electronic withdrawal limit your liability for unauthorised transactions may increase.

23. When are electronic transactions (including BPAY) processed?

Electronic transactions on most accounts are generally processed on the day they are made or scheduled to occur (Sydney/Melbourne time). However, due to processing requirements, a funds transfer from your account made via *Internet Access* between 12:00 midnight and 12:30 am (Sydney/Melbourne time) on Sunday to Friday (inclusive), or transactions made between 12:00 midnight and 1:30 am (Sydney/Melbourne time) on a Saturday, may be treated as if the transfer occurred on the next *Business Day*.

Payments to accounts at other financial institutions will be credited to the recipient's account when the other financial institution processes the transaction, which may take up to 3 *Business Days*.

For security reasons we may place a hold on funds transferred to or from your account. The hold may apply for as long as we reasonably need to investigate the transaction.

24. BPAY

If we conclude that your account has been incorrectly debited or credited, we will, where

appropriate, adjust your account (including any interest and charges) and let you know in writing of the amount with which your account has been debited or credited.

If we reasonably conclude that your account has been correctly debited or credited or, in the case of unauthorised transaction, that you are liable for the loss or part of the loss, we will give you copies of any document and/or other evidence on which we based our finding.

If any BPAY payment was made as a result of a mistake by you and, after 20 *Business Days* we are unable to recover the payment from the Biller or any other person who received it, you should then pursue the matter with the biller or the person receiving the payment.

In addition, your terms of conditions of your account outline how BPAY payments are handled and recovered.

We are not liable if any retailer refuses to accept a *Debit Card*, PIN, *Password* or other code.

25. You must report the loss, theft or misuse of your *Debit Card*, device, PIN, *Password*, or *Customer Number*

Even if you are confident that codes are secure you must tell us as soon as you become aware of the loss or theft of an access method or of any unauthorised access to your account(s).

26. What happens if I don't report loss, theft or misuse?

If it can be shown that you unreasonably delayed telling us of the loss, theft or misuse of your *Debit Card*, device, PIN, *Password*, *Customer Number* or other codes, or electronic equipment, then you will be liable for unauthorised transactions that occur on your account.

We do not hold you liable for any unauthorised transactions that could have been stopped if you tried to call and report and we weren't available at the time you tried to report the loss, theft or misuse.

However, you should try and telephone us again as soon as possible.

27. Ensuring the security of your *Debit Card*, devices, PINs, *Password*, *Customer Number* or other codes

If we reasonably believe your *Debit Card*, PIN, *Password*, other code or device is being used in a way that may cause losses to you or us, we may cancel or withhold its use at any time, without notice.

We may cancel your *Debit Card* if it is not used for 6 months or more.

Before using your *Debit Card* that hasn't been used for 6 months or more, you should contact us to ensure that it is still activated.

A *Customer Number* may be permanently cancelled by us without notice to you if:

- (a) it has not been used for 12 months or more; or
- (b) it has been suspended by *Origin MMS* for security reasons (for example, because an incorrect *Password* was entered) and you do not contact *Origin MMS* within a reasonable time to arrange for a *Password* change and for the *Customer Number* to be reactivated.

If *Origin MMS* cancels a *Customer Number*, the *Internet Access* service to which it relates will be closed without notice to you. If following cancellation, you want to continue to use the *Internet Access* service, you can

again register for the service by contacting us.

Section 3: Disputes

28. What to do if you have a complaint

We accept that sometimes we can get things wrong, and when this happens, we're determined to make them right again.

29. Talk to us

Most problems can be resolved quickly and simply by talking with us. You can call our Customer Services Team on 1300 767 063.

30. When you make a complaint

(a) When you make a complaint to us we will:

- (i) acknowledge your complaint and make sure we understand the issues;
- (ii) do everything we can to fix the problem;
- (iii) keep you informed of our progress;
- (iv) keep a record of your complaint;
- (v) give you our name, a reference number and contact details so that you can follow up if you want to; and
- (vi) provide a final response within 21 days or advise you of the need for more time to complete the investigation.

(b) Unless there are exceptional circumstances, we will complete our investigation within 45 days of receipt of your complaint. If we are unable to provide a final response to your complaint within 45 days, we will:

- (i) inform you of the reasons for the delay;
- (ii) advise of your right to complain to the Australian Financial Complaints Authority (AFCA); and
- (iii) provide you with the AFCA contact details.

31. External dispute resolution

If an issue has not been resolved to your satisfaction, you can lodge a complaint with the Australian Financial Complaints Authority, or AFCA. AFCA provides fair and independent financial services complaint resolution that is free to consumers. AFCA's contact details are set out below.

Australian Financial Complaints Authority

Website: www.afca.org.au

Email: info@afca.org.au

Phone: 1800 931 678 (free call)

By post: GPO Box 3

Melbourne VIC 3001

32. Disputes with other parties

We are not liable if any retailer refuses to accept a *Debit Card*, PIN, *Password* or other code.

Unless required by law, we are not responsible for the goods and services a retailer supplies to the user. If the user has any disputes, they must be resolved with the retailer. We are also not responsible for complaints with respect to the goods and services a retailer supplies to the user if incorrect charging occurred.

You must ensure that the correct amount has been entered in the electronic equipment before authorising the transaction.

Unless you can provide satisfactory evidence to the contrary, you agree that:

- (a) the amount shown on a sales voucher or any other evidence of a purchase is sufficient evidence of the purchase;
- (b) the amount shown on a cash withdrawal voucher, receipt or any other evidence of a cash withdrawal is sufficient evidence of the cash withdrawal; and
- (c) the above applies regardless of whether the voucher or other evidence is signed by you.

You should pursue any disputes over incorrect charging with the retailer.

33. Safeguarding your account against unauthorised access

Access methods comprise the access to your account. You must do everything you reasonably can to protect all means of access to your account. That means making sure your *Debit Card*, devices, *Customer Numbers*, PINs, *Passwords* and other codes and electronic equipment are not misused, lost or stolen or disclosed to any account access service other than your *Origin MMS* Internet Access.

You may suffer loss if you don't sufficiently safeguard these items.

34. Liability for transactions

Generally speaking, you are liable for any losses arising from the acts and omissions of all users. This includes you and any person authorised by you to carry out electronic transactions on your account. You will be liable for:

- (a) transactions carried out by you or someone else with your knowledge and consent; and

- (b) unauthorised transactions if you or any other user have not made a reasonable attempt to disguise or prevent unauthorised access to a PIN, *Password* or other code.

35. Unauthorised transactions

An unauthorised transaction is one which is not authorised by a user, for example a transaction which is carried out by someone besides you without your knowledge and consent.

The *ePayments Code* governs certain electronic payments to or from your account (e.g. electronic transaction payments and BPAY). The *ePayments Code* does not apply to internet access for business accounts.

We will use reasonable endeavours to comply with the *ePayments Code* when our dealings with you fall under that code.

The terms and conditions applicable for your account, provide further details on how your accounts operate and your liability for transactions undertaken on your account.

36. Customer information and Privacy

Personal and transactional information will only be disclosed to: *Origin MMS*; BPAY Pty Ltd; the Billers nominated by you; these Billers' financial institutions; any agent appointed by BPAY Pty Ltd to provide the electronic systems needed to implement the BPAY Scheme (e.g. Cardlink Services Limited). *Origin MMS* does not store the personal information you provide to register with BPAY View with a particular Biller. You can request access to your personal and transactional information held by the *Origin MMS*, BPAY Pty Ltd or its agent, Cardlink Services Limited.

For information about our information collection practices, please see our Privacy Policy available on our website at <http://www.originmms.com.au/privacy->

[policy](#).

Our Privacy Policy contains information on how we process your personal information under the *Privacy Act 1988* (Cth) and the Australian Privacy Principles and your rights under the *Privacy Act 1988* (Cth) in relation to any personal information that we process in connection with providing you with *Internet Access* services.

Our policy should be read in conjunction with the privacy disclosures we give you when you apply for any of our products or services.

Our policy includes information about:

- (a) the ways we may collect, use or exchange your information;
- (b) how you may access and seek correction of the information; and
- (c) how to make a complaint about a breach of your privacy rights, and our complaint handling procedures.

37. Collection of Personal Information

When you use *Internet Access*, we may collect your personal information (including your location) to provide you with our *Internet Access* services and to verify your activity for security purposes.

Origin MMS has a general duty of confidentiality towards you, except in the following circumstances:

- (a) where disclosure is compelled by law;
- (b) where there is a duty to the public to disclose;
- (c) where the interests of *Origin MMS* require disclosure; and

- (d) where disclosure is made with your express or implied consent.

38. Disclosure

We may disclose your personal information to other members of *Origin MMS* Group, anyone we engage to do something on our behalf, and other organisations that assist us with our business. As a provider of account and credit products and services, we have legal obligations to disclose some personal information to government agencies and regulators in Australia, and in some cases offshore.

We may disclose your personal information to an entity which is located outside Australia. Details of the countries where the overseas recipients are likely to be located are in our Privacy Policy.

39. Contact us

If you are not satisfied with how we may handle your personal information or you would like to make a complaint you can contact our Privacy Officer by, calling our Customer Services Team on 1300 767 063 or writing to us at PO Box A1244, Sydney South NSW 1245.

40. Updating your contact details

- (a) **Email address**
You need to keep your email address current. You may update your email address by contacting us. If you don't provide us with a correct email address, we may not provide you with *Internet Access* because you may not receive important information regarding your accounts from us.
- (b) **Mobile phone number**
We may use your mobile phone number to send you SMS Codes and any information relevant to your *Internet Access* service.

When you're registered for SMS Code, you need to contact *Origin MMS* on the number(s) at the beginning of these terms and conditions to update your mobile phone number.

You will be notified of any changes to our records of your mobile phone number via an SMS to both your old and new mobile phone numbers. If you don't provide us with your correct mobile phone number, you may not be notified of important information relevant to the use of SMS Codes.

You need to keep your mobile phone number current. If you update or no longer use your mobile phone number, you must contact us and you may need to re-register for the *Internet Access* services that we provide.

41. Meaning or words

- (a) **Business Days** means a day that is not:
 - (i) a Saturday or Sunday; or
 - (ii) a public holiday, special holiday or bank holiday.
 - (iii) in the place in which any relevant act is to be done or may be done.
- (b) **Customer Number** is the 8 digit number you are given by *Origin MMS* which must be entered into *Internet Access* to identify you.
- (c) **Debit Card** means the *Visa Debit Card* issued to you by *Origin MMS* and Indue Ltd, subject to the *Conditions of Use of Visa Debit* as provided to you with your *Visa Debit Card*.
- (d) **ePayments Code** regulates consumer electronic payments, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking, and BPAY and is published and

monitored by the Australian Securities and Investments Commission.

- (e) **Internet Access** means the online internet access services registered in the name of an individual to manage their accounts online.
- (f) **Origin MMS** means Origin Mortgage Management Services a trading name of Columbus Capital Pty Limited ACN 119 531 252 (Australian Credit Licence 337303).
- (g) **Password** means a confidential alphanumeric containing 8 characters. When used with your Customer Number to access your *Internet Access services*.
- (h) **Prohibited Person** is a person who appears to us either:
 - (i) to be a proscribed person or entity under the Charter of the *United Nations Act 1945* (Cth);
 - (ii) to be in breach of the laws of any jurisdiction relating to money laundering or counter-terrorism;
 - (iii) to appear in a list of persons with whom dealings are proscribed by the government or a regulatory authority of any jurisdiction; or
 - (iv) act on behalf, or for the benefit of, a person listed in subclauses (a) – (c).

42. Severance

If any part of any of these terms and conditions is found to be void or unenforceable for unfairness or any other reason (for example, if a court or other tribunal or authority declares it so), the remaining parts of these Condition of Use will continue to apply as if the void or unenforceable part had never existed.