

## Terms of Use

### Information Technology

#### I. PREFACE

1. Attvest Finance Pty Ltd (ABN: 37 169 039 221) (**Attvest**) provides credit facilities to its customers for the funding of insurance premiums. Attvest provides additional and ancillary services related to funding of insurance premiums and the management of financing insurance contracts. Attvest owns and operates the website [www.attvest.com.au](http://www.attvest.com.au) (**website**) and other forms of information technology communications, systems and software in order to inform people of its services and to provide and manage those services utilising information technology, including proprietary information technology systems.
2. By making use of any of Attvest's services, including its website, OLA processes, ATTtransact and all forms of information technology communications and systems (**InfoTech**), you and the person you represent (if applicable) agree to the use of such services and the InfoTech under these terms of use (**Terms**), which incorporates by reference the relevant parts of Attvest's Code of Conduct and Attvest's Privacy Policy, and as varied, supplemented or amended by subsequent contracts should you decide to enter into such contracts with Attvest.
3. By accessing the website and the materials and information within, using Attvest's InfoTech or by communicating or transacting with Attvest or otherwise engaging with Attvest for information or quotations or transactions or otherwise, you acknowledge that you have read, understood and agree to be bound by these Terms, and any changes to these Terms as they occur from time to time.

#### II. WEBSITE

4. These Terms govern your use of the website, any other web domains owned by Attvest, and any pages linked to the Attvest website or other web domains owned by Attvest (**External Sites**).

##### A. Warranty

5. The materials on the website have been prepared for general information purposes only. Whilst Attvest has used reasonable efforts to ensure that information is free from error, Attvest does not warrant either expressly or impliedly the accuracy or completeness of any materials on the website.
6. Attvest reserves the right to alter, move, modify or remove any content at its absolute discretion from time to time without notice, and is also under no obligation to provide you with alternative links or avenues to such content.
7. Attvest does not warrant that the Attvest website will be free from viruses or anything else that may either interfere with or damage the operation of your computer systems, or that access to the Attvest website or any External Site will be uninterrupted. Under no circumstances will Attvest be liable to you or any third party for damages or interferences to computer systems arising out of connection or usage of the Attvest website or an External Site, as well as disruptions experienced whilst using the Attvest website.
8. You must take your own precautions to ensure that whatever you select for use from the website is free of viruses or anything else that may either interfere with or damage the operation of your computer systems.

##### B. Limitation of Liability

9. Except for the rights, guarantees and remedies which cannot be excluded, restricted or modified, to the maximum extent permitted by applicable law Attvest excludes all liability incurred, suffered by or awarded against you under or in any way as a result of your use of or reliance upon the website or the content contained herein.
10. As per our choice under the *Competition and Consumer Act 2010* (Cth), Schedule 2 – section 64A, Attvest excludes all and any liability which may arise for any damages, losses, liabilities, expenses, costs or consequences of any nature including without limitation loss of revenue, claims and expenses suffered by you or any third party.
11. In no event shall Attvest's total liability to you for all damages, losses, and causes of action exceed the amount paid by you, if any, for accessing the website, even if Attvest has been advised of the possibility of such damages.

##### C. Copyright and Intellectual Property Rights

12. The material contained on the website is protected by copyright, with all rights reserved by Attvest. You may use the website only for your personal and non-commercial purposes without further or additional permission. You may use the website for business purposes only where specifically permitted by Attvest. No term or condition stated on the website will express or imply approval for commercial purposes.
13. Trademarks (whether registered or unregistered) and logos belonging to Attvest or third parties whom have agreed to the display of their trademarks and logos must not be used in any way without obtaining the express prior written consent of Attvest. At no time can such trademarks be modified by you. The content contained in the website may be the subject of other intellectual property rights owned by Attvest or by third parties. No licence is granted in respect of those intellectual property rights other than as set out in these Terms. Your use of the website must not in any way violate or infringe upon the intellectual property rights of any person or entity.

#### **D. Rights of Material**

14. You are granted a revocable license to download the material contained on the website for your personal use, as well as for the purpose of transacting business with Attvest. You must not otherwise copy, reproduce, republish, frame, upload, transmit, redistribute or modify the contents of the website or any document published therein in any way, except where the prior written consent of Attvest has been obtained.

#### **E. External Sites**

15. The website may have been linked by or contains External Site links to, or frame, websites of third parties. Attvest is not required to either maintain or update any links on the Attvest website. Attvest is not authorising the reproduction of External Site material by linking material on the website to External Site material.
16. Links to, or framing of, External Sites should not be construed as any endorsement, approval, recommendation or preference by Attvest of the copyright holders, site or content owners, operators of the External Sites, or for any information, products or services referred to on the External Sites unless expressly indicated on the website.
17. Attvest makes no warranties or representations whatsoever in relation to any aspect of External Site material, including the quality, appropriateness or accuracy of any information or the products and services available through External Sites. Attvest accepts no liability, or responsibility, in relation to material contained on External Sites whether linked to, or framed, directly or indirectly.

#### **F. Security**

18. Attvest makes no warranty in respect of the strength or effectiveness of the security methods or technologies provided both directly within the Attvest website and between the Attvest website and your own system. Attvest is not responsible for any events arising from unauthorised access to the information you provide, utilise or access on the Attvest website.

#### **G. Links to Attvest**

19. No terms contained in these Terms will imply authorisation for any party to create links to the Attvest website. If you wish to create a link to any part of the website, you must obtain prior written consent from Attvest before doing so.
20. To obtain consent, send e-mail to [service@attvest.com.au](mailto:service@attvest.com.au) stating:
  - (a) Your Name
  - (b) Company Name
  - (c) Contact details, including phone and e-mail
  - (d) URL of any (and all) sites you intend to link from
  - (e) Nature of your business
  - (f) Explanation of the purpose of the links and context within which the links will appear
  - (g) Description of how the links will work – e.g framed / direct link
21. Attvest will assess each request on a case by case basis and will notify you of approval if granted.

#### **H. Information submitted by you**

22. All information submitted to Attvest through the Attvest website, including any cookies or other analytics objects, will be deemed to be the property of Attvest. By submitting any information to us through the Attvest website, you grant us an unrestricted, irrevocable license to use, display, reproduce, modify, perform, transmit and distribute that information. You also agree that Attvest is free to use for any purpose any ideas, concepts, know-how or techniques that you submit to us through the Attvest website.
23. Attvest is not subject to any obligations of confidentiality regarding submitted information, except where Attvest has a direct customer relationship or as otherwise specifically set out in these Terms or required by law.

#### **III. ATTtransact**

24. These Terms govern your use of ATTtransact, whether or not ATTtransact is used or accessed directly or through the website or as an embedded InfoTech component of any services provided by Attvest.
25. The ATTtransact system is an integral component of Attvest's InfoTech. ATTtransact includes a proprietary payments and receipting system underlying Attvest's transactions and which facilitates and enables Attvest's service provision, including background and other funding methods, payment arrangements, payment methods, collection of outstanding insurance premiums and settlements of insurance premiums, related receipting and bank reconciliations and electronic communications and data processes.
26. ATTtransact makes use of proprietary InfoTech and the banking and financial transaction services of an authorized deposit taking institution, namely Australia and New Zealand Banking Group Limited (ANZ), in relation to money transactions. ATTtransact and any Attvest entity referred to in the Terms is not an authorised deposit-taking institution for the purposes of the Banking Act 1959 (Cth) and its obligations do not represent deposits or other liabilities of ANZ. ANZ does not guarantee or provide assurance in respect of the obligations of that entity, unless stipulated under the law or noted otherwise. For further details about the operation of your bank account(s) and other information about banking products and services, please read the Product Disclosure Statement associated with your bank accounts.
27. For the purposes of these Terms, Transaction or transaction includes each utilisation of Attvest's services or engagement with Attvest, such as for money transaction or information purposes, using Attvest's InfoTech.

## **A. Important information**

28. You are responsible for any fraudulent or unauthorised transactions or communications. Attvest is only responsible for fraudulent or unauthorised transactions or communications that arise as a direct consequence of a fraud or failure of a contractual obligation on the part of Attvest. No obligation is created and no expectation arises (and is, in any event, excluded) with regard to ATTtransact and other elements of Attvest's InfoTech in respect of confirming or verifying the details, including banking details, of the user or intended recipient of such services. ATTtransact relies on the accuracy and veracity of the information and details entered on the system by you or for you as a user of the system under these Terms. For example, if the person ordering a payment (whether you or your client or the insurer, as applicable) uses bank account details of a third party (who did not authorise the transaction) and the money has been released to an incorrect recipient, then the person ordering the payment is liable for accounting to the actual intended recipient, such as the client or insurer (if applicable) or that third party for the amount of the payment and regardless of whether Attvest or the ATTtransact or other Attvest InfoTech could have sought additional or other verification or confirmation from you or the actual intended recipient.
29. In order to reduce the risk of fraud and potential cost to you or your client (if applicable), we recommend you consider the following information and take appropriate steps following any professional advice you may require when considering such information.
30. **Identity theft –**
- (a) Identity theft happens when a criminal steals personal information and uses it to commit a crime such as opening fraudulent loans or stealing money from you or your bank accounts.
  - (b) Cybercriminals can steal information including contact details, tax file numbers, credit card details, Medicare card details, online account usernames and passwords.
  - (c) Some of the signs of possible identity theft include:
    - (i) your bank transaction history shows purchases or withdrawals you have not made or authorised.
    - (ii) you stop receiving mail or stop receiving regular, expected mail like your utility bills.
    - (iii) you start receiving communications related to a credit facility you did not open or authorise to be opened.
    - (iv) a government agency gets in touch regarding a benefit that you have not applied for or your agent did not apply for on your behalf.
    - (v) you start receiving calls from debt collectors without being behind in loan repayments.
  - (d) Some of the ways you can minimise the likelihood of having your identity stolen include:
    - (i) limit what you share online.
    - (ii) set your social media privacy settings to "private".
    - (iii) do not accept new connections on social media from people you don't know.
    - (iv) be suspicious of communications asking you to confirm sensitive personal information.
    - (v) use strong, unique passwords for each online account.
    - (vi) keep your devices, applications and operating system patched and up to date.
31. **Malware –**
- (a) Malicious software, or "malware", can be used by cybercriminals to:
    - (i) remotely access your computer or smart device
    - (ii) use your computer to attack a third party
    - (iii) install additional software on your software including ransomware
    - (iv) attempt to log keystrokes and capture sensitive information while the user is typing
    - (v) access the microphone and/or webcam on a user's device.
  - (b) Malware can infect your device through a variety of methods such as:
    - (i) opening a suspicious file
    - (ii) clicking on a link to a malicious website
    - (iii) installing modified software that's been shared for free on the internet
    - (iv) opening a Microsoft Office document with macros embedded in them.
  - (c) If you have been affected by malware, you might notice your device is running slower than usual, ads popping up on your machine you did not expect or notice websites asking for more details than they normally do to do something like logging in. You may also notice alerts from your anti-virus software telling you about an infection.
  - (d) Some of the ways to reduce your risk of being affected by malware include:
    - (i) use anti-virus software and keep it updated.
    - (ii) make sure your applications and operating systems are up to date.
    - (iii) regularly back up your files.
    - (iv) use strong passwords.
    - (v) disable Microsoft Office macros by default and only use macros you know and trust.
    - (vi) regularly run anti-virus scans of your machine and review installed applications for unusual items.
    - (vii) do not download applications from third-party download sites or peer-to-peer networks.
    - (viii) do not click on online ads to download applications.
32. **Online threats –**
- (a) Use strong, unique passwords and change your password if you believe it may have been compromised. Adopt two-factor authentication for your important accounts to add an extra layer of security. Attvest's OLA service and other Attvest InfoTech, such as ATTtransact, includes a mobile device security process which utilises actionable push notifications to verify activity.

- (b) Install an anti-virus software and keep it updated to reduce the likelihood of being impacted by malware.
- (c) Regularly back up your computer and devices.
- (d) Think before you share information on social media, especially personal information such as the address of your new house in a photo.
- (e) Be aware of phishing emails and do not click on them.

**33. Payments and other money transactions –**

- (a) Order the payment or authorise the transaction only after you have verified the intended ultimate recipient's bank account details.
- (b) Insist the intended payee is the same person(s) who is listed as the payee on the contract or invoice, or sufficiently satisfy yourself of the connection between the bank account holder and the payee (and the associated fraud risk).
- (c) Identify the payee, intended payer and your client (if applicable), provide verification of this to Attvest using Attvest's mobile device security process and keep records of this.
- (d) In addition, there may be consequences for either yourself, your client (if applicable) or the insurer under the insurance contract or at law if payments are recalled / dishonoured, misdirected or delayed – you should satisfy yourself of the legal ramifications associated with this (e.g. Attvest or the insurer may be entitled to terminate the contract, or impose additional costs – and parties may seek to involve you or hold you responsible for further or additional payments).

**34. Phishing attacks –**

- (a) Phishing emails often impersonate organisations or government agencies. They may contain a link asking you to enter your information or to respond quickly to their request via email.
- (b) Be on the lookout for poor spelling, grammar or other errors in the email that don't match the organisation's presentation.
- (c) Be suspicious of emails with offers that seem too good to be true or that threaten you to take an action they have proposed.
- (d) If you were not expecting a message from a person or business, do not click on the links or open attachments to an email. You can always reach out to the person or business via another communication channel to verify the legitimacy of the message you have received.
- (e) Before you click a link, hover over it to see the actual web address it will take you to. If you don't recognise or trust the address, you can always search for the article or site via a search engine with relevant key terms the page might use.
- (f) Utilise a spam filter to block suspicious messages from reaching your inbox.
- (g) Remember, we will never ask you for your passwords or secure codes via email.

**35. Phone scams –**

- (a) You may receive scam calls even if you have a private number or are registered on the Australian Government's Do Not Call Register.
- (b) Never disclose your personal information, financial account or online account details over the phone unless you made the call and got the number from a reliable source or you verified the caller by utilising a two factor authentication process you set up with your service provider.

**36. Private browsing –**

- (a) If you usually use private browsing, note that you will need to turn off private browsing in order to log in to or use certain Attvest InfoTech systems.

**37. Phone Fraud –**

- (a) Fraudsters may illegally port your phone away from you. Phone porting fraud is when your mobile phone number is ported to a new telecommunications (telcomms) provider without your consent. Phone porting is a legitimate and required service offered by telcomms providers to enable phone users to change telcomms providers while retaining their phone numbers and connected accounts, related apps and two-factor authentication methods. A phone port can be initiated by providing the genuine owner's name, mobile number, email, or date of birth.
- (b) If your phone number has been illegally ported, you may lose mobile phone reception, access to network data and therefore, the ability to call and text.
- (c) The fraudster who illegally ported your number can now text, make calls from your phone number and is the new "owner" of the number registered for your two-factor authentication. This means, the fraudster can log into your internet banking by using your mobile phone number to reset your password and then transact on your accounts.
- (d) Besides porting your phone, a fraudster may cause a SIM swap.
- (e) A SIM swap is where the fraudster will contact your telcomms provider and request to activate a new SIM card with your number. They can do this through the same methods used to port your phone as telcomms providers must swap out damaged or lost or defunct SIMs for their customers.
- (f) In order to carry out a phone porting or SIM swap, a fraudster may have obtained your information through a number of different ways.
- (g) You may have clicked a phishing link through an email or text message and entered sensitive information, or your emails may have been compromised.
- (h) The fraudster may have accessed personal information you may have provided openly on social media profiles. The fraudster may have also accessed this information via "social engineering" through a phone call or messaging app. 'Social engineering' is the act of manipulating people to give up confidential or sensitive information.

**38. Unusual activity to be aware of:**

- (a) your service is suddenly disconnected and showing “SOS only”.
- (b) unexpected texts from your provider advising that you have requested your number to be ported to another network or you have requested a SIM swap.

**39. Consider other steps, such as:**

- (a) removing your email, mobile number, and date of birth from your social media profiles.
- (b) setting up two factor authentication when you or your agent first establishes a relationship with a legitimate service provider.
- (c) being security conscious on social media sites and online.
- (d) using two-step verifications to log into your email account and banking apps.
- (e) never clicking a link you receive via email or text message.
- (f) being aware of cold calls where a scammer will manipulate you to give up personal information such as your banking credentials, credit card, address, or date of birth.

**40. Contact your telcomms provider for more information about increasing your security questions to unique answers only you would know and if you suspect illegal porting of your phone or SIM swap:**

- (a) contact your mobile phone provider immediately.
- (b) contact your financial institution/s.
- (c) contact Attest.
- (d) change your passwords to online banking, email and social media accounts.
- (e) for help with identity fraud, contact ID Care.
- (f) report the matter to your local police.

**41. Ransomware –**

42. Ransomware is a type of malware that locks your device and its files so you cannot use them without paying a ransom.

43. Ransomware can be very costly and you may not be able to recover your data or your system. Ransomware commonly uses encryption techniques to lock your files, making them unreadable, and some go one step further and make your device unusable.

44. Ransomware infects users’ devices through the same techniques as malware and can include:

- (a) opening a suspicious file sent to you
- (b) clicking on a link to a malicious website
- (c) installing modified software that’s been shared for free on the internet
- (d) opening a Microsoft Office document with macros embedded in them.

45. The Australian Cyber Security Centre’s guidance does not recommend paying the ransom if you are affected by ransomware. There is no guarantee that paying the ransom will get your files back or your computer fixed. You should engage an expert professional technician for assistance if you are affected.

46. Some of the ways to reduce your risk of being affected by ransomware include:

- (a) use anti-virus software and keep it updated.
- (b) make sure your applications and operating systems are up to date.
- (c) regularly back up your files.
- (d) use strong passwords.
- (e) disable Microsoft Office macros by default and only use macros you know and trust.
- (f) regularly run anti-virus scans of your machine and review installed applications for unusual items.
- (g) do not download applications from third-party download sites or peer-to-peer networks.
- (h) do not click on online ads to download applications.

**47. Technical support scams –**

- (a) Technical support scams involve cybercriminals getting in contact with users and pretending to have identified a serious problem with the user’s computer or internet connection and offer to help. They’ll ask for remote access to the user’s computer but in doing so, will access files, intercept bank account logins and other sensitive information on the machine. They may also ask the user to pay a fee to fix the machine.
- (b) This scam works on intimidating the user, often using technical words and phrases to confuse the victim and employing techniques to build urgency. The scams can be initiated via a cold call, mass-messaged emails to users or via pop-up ads suggesting you’ve got a virus and to call a 1800 number for help.

48. Some of the ways you can protect yourself from scams such as these include:

- (a) always keep your computer up to date with the latest software updates, antivirus software and a good firewall.
- (b) never disclose your personal information, financial account or online account details over the phone unless you made the call and got the number from a reliable source or you verified the caller by utilising a two factor authentication process you set up with your service provider.
- (c) if a stranger asks for remote access to your computer just say “no”, even if they claim to be from a reputable business.

## **B. Supported technology**

49. The website and ATTtransact and Attvest InfoTech is designed to run on a broad range of browsers and operating systems, and on a range of popular devices including most smartphones, tablets and computers.
50. **Optimum browsers –**
- (a) Firefox 23 or greater
  - (b) Chrome 24 or greater
  - (c) Safari 8 or greater
  - (d) Internet Explorer 10 or greater
  - (e) Edge 20 or greater
51. You can use the links following to download the following browsers:
- (a) Internet Explorer from <http://www.microsoft.com/windows/downloads/ie/getitnow.mspx>
  - (b) Firefox from <http://www.mozilla.com/firefox/>
  - (c) Google Chrome from <https://www.google.com/intl/en/chrome/browser/>
  - (d) Safari from <http://www.apple.com/safari/download/>
52. **Optimum mobile operating systems –**
- (a) iOS 5.x or greater
  - (b) Android 4.4 or greater (i.e. KitKat 4.4+, Lollipop 5.0+ and marshmallow 6.0+)
53. Note that the following devices are specifically not supported:
- (a) Windows mobile
  - (b) Blackberry
54. Operating systems, device operating systems and browser combinations can be quite diverse and we may not be able to check our sites work on some of the more unique combinations, so if you find an issue with your particular set up, please let us know and we can investigate.
55. **Security –**
- (a) All information within the website, including ATTtransact, is protected by 256-bit encryption running on a Secure Socket Layer (SSL). You can confirm your session is encrypted by the appearance of a locked padlock symbol at the foot of your browser.

## **C. Ways to protect yourself**

56. It is important to secure your computer properly to prevent putting yourself, your business and possibly your family and friends at risk. There are simple measures you can take to protect your computer and your personal information. Bear in mind information technology systems, the worldwide web, the internet, e-mails, social media, mobile phones and all electronic forms of communication and storage are inherently at risk of compromise, corruption or failure and there are no guarantees that you will avoid or transfer the risks of transacting and engaging with Attvest using information technology and electronic media.
57. **A strong password –** A good password should be at least eight characters and contain a mix of letters, numbers and symbols in upper and lower case. Avoid using your name, username or something easily identifiable. Remember to use different passwords for logging into different sites and change your passwords regularly. If you believe your password may have been compromised change it as soon as possible and let us know of the changes.
58. **Anti-spyware –** Spyware is a form of online snooping. You can help prevent spyware by using up-to-date anti-spyware software
59. **Anti-virus software –** Up-to-date anti-virus software is key in helping prevent online threats and protecting your details while performing online financial transactions.
60. **Auto-fill –** Most browsers have a native autofill feature. This is not disabled on Attvest InfoTech sites, but when using this feature for credit card details, please follow the security guidelines of your browser to keep your details safe.
61. **Operating system –** Regularly check your operating system is up-to-date. (You can do this by ensuring “auto updates” are enabled.) This will help protect you against online security threats such as malware.
62. **Scams awareness –** Learn how to protect yourself from scams with using in-depth scams awareness pages and articles published by your bank, your insurance company and government agencies:
- (a) [For help with protecting yourself online and reporting cybercrime ReportCyber](#)
  - (b) [eSafety commissioner](#)
  - (c) [IDCARE, national identity and cyber support](#)
  - (d) [Stay Smart Online. The Australian Government’s cyber security website](#)
  - (e) [Scam Watch, a website operated by the Australian Competition and Consumer Commission \(ACCC\)](#)
  - (f) [The consumer section of the Australian Securities and Investments Commission \(ASIC\)](#)
63. **Web browser –** An up-to-date web browser will help protect you against security threats such as malware. The latest browser version can be downloaded from your browser providers’ website.
64. **Wireless connection –** If you are using a home wireless network, make sure this has been set up securely. If you are using a third party network, ensure you only use a trusted and secure wireless network connection.
65. When in doubt seek independent expert and professional help before proceeding.

#### **D. Specific money transaction user obligations**

66. Before making ATTtransact available for prospective payers or using ATTtransact money transaction payment enablement you or your client (if applicable) as payer must ensure:
- (a) you have a portable device from which you can authenticate ATTtransact transactions, and that your portable device can connect to a secure internet connection and the mobile telephone network and is operated by you or on the payer's behalf by a person duly authorized thereto.
  - (b) you have a device with which you can conduct ATTtransact transactions, and that your device can connect to a secure internet connection and is operated by you or on your behalf by a person duly authorized by you; and
  - (c) that the payee has agreed to payment through ATTtransact to the nominated bank account of the payee and understands that funds can take up to three (3) Business Days to clear and be received by the payee.
67. If paragraph 66 is satisfied, you can elect to pay using a payment method enabled or facilitated by ATTtransact.
68. ATTtransact is not the only method of payment, it is an embedded system to facilitate electronic transactions including various methods of payments, and you agree that (and you undertake to notify your clients, if applicable) while the use of ATTtransact is not always optional, you select the payment method of your own free will and that there are other payment options available to you (or them, if applicable) to pay besides those that may be available as part of ATTtransact.
69. You should verify the identity of each payer and payer account details and the payee and payee account details (as the case may be). The account holder should match the name of the payer or payee (as the case may be) on the contract or invoice (or you should be sufficiently satisfied of the connection if different).
70. You are responsible for ensuring the accuracy of the details, the amount, the payer and payee and all other information and details required to facilitate a successful transaction, including payments.
71. You must ensure that you, or the payer if you are acting for a payer, is provided with sufficient opportunity to read the ATTtransact Money Transaction Authority, and that they have willingly agreed to those terms prior to making payment using ATTtransact.
72. On each occasion that you present or offer or use ATTtransact to facilitate money transactions, you represent and warrant that you have successfully met each requirement described in this section D.
73. For the purposes of money transaction user obligation, the following words have the following meanings:
- (a) **ARN** stands for "ATTtransact Reference Number", a unique number issued to you in order for you to transact via ATTtransact. The ARN assists you to identify payers, payments, reconcile accounts and utilise Attvest's services using Attvest's InfoTech services.
  - (b) **ATTtransact Money Transaction Authority** means these Terms and the Attvest Direct Debit Authority and the Attvest Credit Card Authority and the Attvest Alternate Electronic Payment Authority (as applicable and as the case may be).
  - (c) **Dishonoured** means the process where the payer's financial institution, either on its own or on instruction from the payer, requests that a charge or direct entry (electronic) transaction be reversed back to the payer's financial institution for any reason.
  - (d) **Full Recourse** means the right to recover payment from the Agent for a transaction as set out in these Terms, which may be against any accounts of the Agent in debit or credit.
  - (e) **payee** means any person(s) to whom payment is ordered by a payer using a valid ARN to transact via ATTtransact, whether in payment or receipt of insurance proceeds, insurance premium funding, insurance contracts or otherwise in connection with related or ancillary Attvest services.
  - (f) **payer** means any person(s) who uses a valid ARN to order a payment to a payee via ATTtransact, whether in payment or receipt of insurance proceeds, insurance premium funding, insurance contracts or otherwise in connection with related or ancillary Attvest services.

#### **E. Relationship of parties using ATTtransact money transaction functions**

74. Attvest will –
- (a) act as agent for the Agent for the purposes of:
    - (i) the receipt of monies payable to the Agent by payers, which may include monies owing to the Agent in its own right and in its capacity as agent for any third party (e.g. clients of the Agent);
    - (ii) the payment of monies payable by the Agent, which may include monies owing by the Agent in its capacity as agent for any third party (e.g. insurers of the clients of the Agent);and
  - (b) otherwise act as a principal in respect of its obligations as a service provider in providing ATTtransact as part of its services.
75. You acknowledge that nothing in these money transaction user terms is intended to, nor will it, create:
- (a) a joint venture or partnership between the parties; or
  - (b) any contractual or binding relationship or vicarious duty of care between Attvest and a payer or payee or any other person making a payment to or from the Agent through ATTtransact or using ATTtransact's money transaction functionality.
76. You should verify the identity of each payer. The account holder should match the name of the person on the relevant contract or invoice (or you should be sufficiently satisfied of the connection if different).
77. You are responsible for ensuring the accuracy of the payment details, the amount and all other information required to facilitate a successful payment.
78. If applicable, you must ensure that the payer is provided with sufficient opportunity to read the the ATTtransact Money Transaction Authority, and that they have willingly agreed to those terms prior to ordering payment using ATTtransact.

79. On each occasion that you offer ATTtransact as a money transaction option, you represent and warrant that you have successfully met each requirement described in this section E.

**F. Payment requirements, liabilities and refunds**

80. We will not accept payment from a payer through ATTtransact unless the person making payment produces a valid ARN.
81. Payment of any amount tendered by a payer may be accepted by us pursuant to these Terms, unless amended, modified or varied by another contract between us and the payer.
82. All money transactions must be made by direct debit from a compatible bank account, or by credit card or by another electronic payments method. You must arrange for each payer to provide an appropriate authority in our favour to debit the payer's bank account or other electronic payments method under an ATTtransact Money Transaction Authority.
83. You are responsible for any incorrect or unauthorised amounts debited. To the extent permitted by law, we are not liable to pay you and you indemnify us against any fraudulent or Dishonoured money transactions.
84. In the event that we are unable to perform the agency functions for any reason beyond our control (including force majeure), we will advise you in writing of such inability within a reasonable time.
85. Should you owe an amount back to the payer (e.g. a refund), in order to reduce the risk of fraud and your potential liability for this, you should notify us of the details of the transaction for a refund to be made back to the same account from which the payment was originally made. Do not process any refund directly as you may remain or become liable for losses.

**G. Dishonoured payments**

86. You acknowledge that payments made through or facilitated by ATTtransact may be subsequently Dishonoured at any time after a payment is made.
87. Payments can take up to three (3) Business Days to be received in clear funds, and can be automatically recalled and Dishonoured during this period ("Automatic Dishonours") - for example, because the payer did not have sufficient funds in their bank account. This is distinct from manual Dishonours or "Disputed money transactions", which can arise weeks or months after the initial money transaction and are subject to consultation and investigation.
88. As Automatic Dishonours arise without notice, you should retain the funds in your account until they are cleared (particularly if your payer or destination account is a trust account). For fraud mitigation purposes, we recommend you retain the funds in your account for at least a week after initiating the transaction or a week after the time on which a regular debit order payment is to be made.
89. If applicable, unless you instruct us in writing to draw funds from another account, you authorise us to operate on the bank account linked to ATTtransact for the purpose of processing Dishonoured transactions, even if that account is a trust account.
90. Without limiting paragraph 107, you must ensure that sufficient funds are maintained in your bank accounts to cover any shortfall caused by such Dishonoured payments. You indemnify us against any loss caused by these Dishonoured payments.

**H. Disputed transactions**

91. A money transaction is a "Disputed money transaction" if a payer notifies you or us of a dispute, complaint or query concerning that money transaction.
92. If we notify you of a Disputed money transaction, you must provide us with a written response no later than five (5) Business Days after receipt of such notification. Your response must be substantive and contain a resolution or explanation of the Disputed money transaction, which will enable us to resolve the Disputed money transaction. If such a response is not received by us within five (5) Business Days, we will have Full Recourse against you for the amount of the Disputed money transaction. You must also provide us with any other information relating to the Disputed money transaction that we reasonably request.
93. If a payer notifies you of a Disputed money transaction, you will provide to the payer a written response no later than five (5) Business Days after receipt of such notification. Your response to the payer must be a substantive response containing a resolution or explanation of the Disputed money transaction.
94. If a payer notifies you of a Disputed money transaction and it is determined that the payer be refunded, you should notify us of the details of the money transaction for a refund to be made. Do not process any refund directly as you may remain or become liable for losses.

**I. Fees and charges**

95. You must pay the relevant fee or charge for each money transaction performed via ATTtransact and any other fees as set out in the relevant contract between you and Attvest. Unless stipulated in a relevant contract between you and Attvest there are no fees and charges payable for the use of ATTtransact as an embedded element of the Attvest InfoTech. The maximum amount for money transactions performed via ATTtransact payable by the payer is set out in the Attvest Special Fees, Charges and Surcharges table published by Attvest from time to time.
96. By default and unless a relevant contract sets out something else, any fee or surcharge will be passed on to payers. If you subsequently want to change this position, you may do so by giving us no less than 30 days' written notice.
97. You authorise and instruct us to collect any transaction fees and surcharges payable by you in connection with a money transaction and which will be passed on to payers directly from the relevant payer at the time of the money transaction.
98. You indemnify us in respect of any government duties, taxes and charges in connection with the money transactions payable by you, the payer or any other party in respect of any money transaction.



99. Acting reasonably, we may vary or introduce any fee or charge if we provide you notice in accordance with this section I no later than thirty (30) days before the day that the new fee or charge is intended to take effect.
100. You agree that we can give notice of a variation or introduction of a fee or charge in writing, electronically, by publication on our website or in any other way permitted by law.
101. Information on current standard fees and charges is available on request. Please contact us if you require any further information about fees and charges that are applicable to the use of ATTtransact.

#### **J. Advertising**

102. No party will use the name or logo of the other in any advertising material without the prior written consent of that other party.
103. Any advertising in relation to ATTtransact must not be used without our prior written consent.
104. During the provision of ATTtransact you may, subject to such conditions as we may reasonably impose, include accurate factual references to the existence of ATTtransact in your advertising material and any necessary documentation.

#### **K. Warranties**

105. To the extent that is permissible by law, Attvest disclaims all conditions and warranties, express or implied, in respect of the provision of Attvest's InfoTech.
106. Notwithstanding the terms of this section K, our responsibility under these Terms, as well as for breach of any implied statutory condition or warranty which cannot be excluded will, if any legislation so permits, be limited, in our discretion to:
  - (a) the resupply of ATTtransact; or
  - (b) the cost of resupply of ATTtransact, (including, if applicable, the amount of any money transferred or received as the subject of the money transaction) in respect of which the breach occurred.
107. Attvest's liability under these money transaction terms is limited to the amounts specified in this section K. Therefore, Attvest will not be liable to the Agent and/or payer for, and the Agent will indemnify Attvest against, any action, proceeding, claim or demand relating to any direct or indirect loss or damage which exceeds this limitation. This section K also applies to any loss or damage which results from any act or omission by Attvest of any duty, obligation or function whilst providing ATTtransact.
108. Attvest will, if requested by the Agent, take reasonable steps to assist the Agent in the event of any claims being received by the Agent from a third party where such claim arises directly out of the provision of ATTtransact.

#### **L. Confidentiality**

109. Subject to paragraph 110, the parties will treat as confidential and may not disclose any information which comes into their possession pursuant to or as a result of the provision of ATTtransact.
110. The Agent acknowledges that Attvest may conduct data aggregation and analysis, based on the information we have collected from use of ATTtransact. We may package such information and use it for our own purposes or sell it to interest parties.
111. Confidentiality of charges and prices will be maintained and the Agent may not disclose negotiated charges or prices to a third party without the approval of Attvest.
112. Notwithstanding the terms of this section L, such information may be disclosed if required by any law or order of any court, tribunal or regulatory body.

#### **M. Force Majeure**

113. No party will be liable to the other, nor be in default of these Terms, for failure to observe or perform any provision of these Terms for any reason or cause which could not with reasonable diligence be controlled or prevented by the party in question, provided that the party relying on this paragraph must give notice to the other party of its inability to observe or perform the provisions of these Terms and the reasons for this.

#### **N. Termination**

114. Either party may terminate the supply or use of ATTtransact without cause and without the need to give any reason or explanation, by giving the other party written notice specifying a date for the termination (being not less than 30 days after the date of such notice). Termination of the supply or use of ATTtransact may result in the termination of the supply or use of other or all of Attvest's services.
115. Termination of the ATTtransact service will not relieve either party of its duty to fulfil its obligations under these money transaction terms in respect of any money transaction occurring prior to the termination date.
116. In the event of the termination of the ATTtransact service, the Agent:
  - (a) will not be entitled to any refund of fees and charges paid to Attvest pursuant to this part of the Terms; and
  - (b) indemnifies Attvest in respect of any fees, charges and expenses incurred by Attvest or payable to Attvest in the performance of its obligations under these Terms.
117. Any payments received by Attvest after the termination of the ATTtransact service may, in Attvest's absolute discretion, be Dishonoured or returned to the payer.

#### **O. Suspension**

118. For the protection of the Agent and Attvest, we may suspend your use of ATTtransact without prior notice if:
  - (a) you are in breach of any of your obligations under these money transaction terms;
  - (b) you or anyone acting on your behalf is suspected of being fraudulent; or
  - (c) to otherwise protect our interests.

## IV. MISCELLANEOUS

### A. Assignment

119. While we may assign these Terms at any time and from time to time, the liabilities and obligations contained in these Terms may not be assigned by you without the prior written consent of Attvest.

### B. Code of Banking Practice

120. This is not a banking service and must not be construed as a banking service to which the Banking Code of Practice ("BCOP") applies. The BCOP is an industry code which sets standards of good banking conduct for banks, their staff and their representatives. The BCOP may apply to you if the banks involved in the transaction and providing banking services have adopted the BCOP and if you are an individual or a small business (as defined in the BCOP).

### C. Complaints

121. If you have a complaint or dispute about anything relating to your use of Attvest's InfoTech services, including ATTtransact, you can contact us by:

- (a) contacting your relationship manager,
- (b) calling 1300 363 590, or
- (c) emailing: [service@attvest.com.au](mailto:service@attvest.com.au) and including a full explanation of your situation. We will generally reply within two (2) Business Days.

122. If we do not rectify a problem notified by you under this section C, you may have the option to contact the Australian Financial Complaints Authority ("AFCA"). You can contact AFCA by:

- (a) writing to: Australian Financial Complaints Authority, GPO Box 3, Melbourne VIC 3001,
- (b) calling: 1800 931 678 (free call), or
- (c) emailing: [info@afca.org.au](mailto:info@afca.org.au)

123. AFCA offers an independent and free resolution process of disputes between consumers and financial service providers. AFCA has certain terms of reference that must be satisfied in order for it to investigate your problem.

### D. Interpretation

124. For the purposes of these Terms the following capitalized or emboldened words or phrases have the following meanings:

- (a) **Agent / you / your** means you, the person who will transact, including receiving or making payments, or otherwise use Attvest's InfoTech as described in these Terms. Certain of the terms are only applicable when you become a customer of Attvest or they may apply if you are already a client of an insurance intermediary (such as an insurance broker) or if you are an intermediary (such as a broker) making use of Attvest's InfoTech, including ATTtransact, for your own purposes.
- (b) **Business Day** means every weekday on which Attvest is open for business except for Australian national public holidays.
- (c) **we / us / our** means Attvest.

125. The terms set out under Part II, sections A to E apply to Part III by reference and supplement and add to the terms set out under Part III (and vice versa), and these Terms apply by reference to any use of Attvest's InfoTech, regardless of whether an ATTtransact money transaction occurs or otherwise use of Attvest's InfoTech is made through a website or through an application (**app**) electronic portal, electronic gateway, application programming interface (**API**), electronic mail, closed user network, virtual private network (**VPN**) or by any other electronic information technology means or mode. These Terms must be interpreted to give effect to the agreement by the parties that the parties will only use Attvest's InfoTech in accordance with these Terms as applicable to the relevant information technology application and the other terms of the individual contracts, including Attvest's code of conduct and privacy policy, by and between Attvest and users of Attvest's InfoTech.

### E. Jurisdiction

126. These Terms are governed by the laws of Queensland. By using this site or Attvest's InfoTech, you unconditionally submit to the exclusive jurisdiction of the courts of Queensland and all courts which have a jurisdiction to hear appeals from those courts in respect of all matters or things arising out of these Terms.

### F. Notices

127. Notices and other communications must be signed by the party giving, serving or making the notice or on its behalf by any attorney, directory, secretary, other duly authorised officer or solicitor of such party.

128. Notices and other communications will be deemed to be given, served or made:

- (a) (in the case of delivery by hand) on delivery;
- (b) (in the case of prepaid post) on the third Business Day after the date of posting;
- (c) (in the case of email) on the day of sending (if before 5pm), or on the following Business Day (if after 5pm or if sent on a non-Business Day), provided no automatic email delivery failure notification is received by the sender.

### G. Privacy

129. Attvest acknowledges its obligations under the Privacy Act 1988 (Cth) in relation to personal information provided to it.

130. The Agent warrants to Attvest that it has obtained each user's, payer's or payee's (as the case may be) consent prior to providing Attvest with any personal information relating to the user, payer or payee (as the case may be) and it agrees to indemnify Attvest against any action or claim made by a user, payer or payee (as the case may be) or any other person or authority which relates to the provision or disclosure of this information.

## H. Severance

131. All provisions of these Terms are severable. No provision will be affected by the invalidity of any other provision except to the extent that such invalidity also renders such other provision invalid. In the event of the invalidity of any provision, these Terms will be interpreted and enforced as if such invalid provision were not contained in these Terms.

## I. Variation

132. Acting reasonably, we may change these Terms at any time on at least 30 days' notice:

- (a) if we think the change should be made to meet our legal obligations, to reflect any judgment of a court or tribunal or to reflect any guidance or views of any regulator or external dispute resolution service of which we are a member;
- (b) as a result of any change or anticipated change in circumstances relating to ATTtransact including, for example (and without limitation), changes to our operations, systems or procedures, changes in technology, changes in any relevant law, code or guidance, changes in market or best practice, changes to the risks, costs, features or benefits of ATTtransact, or changes in our structure or financial position;
- (c) if we think the change should be made for reasons of security, to streamline administration, to correct errors, inaccuracies or ambiguities, or because it would be impractical for us to continue without the change; or
- (d) to make the Terms clearer or simpler.

133. Your continued use of Attvest's services after any such change constitutes your acceptance of the revised Terms. If any law regulates that change, we will only make the change to the extent permitted by, and subject to, the requirements of that law.

134. You agree that we can give notice of variations to these Terms, any material change to, or any significant event that affects any of the matters specified in these Terms in writing, electronically, by emailing you or by publishing same on our website or in any other way permitted by law.

135. If requested, you must, on our behalf, give notice to users, payers and payees (as the case may be) of any changes to terms and conditions or fees applying to or affecting users, payers or payees, in the manner and by the time specified by us.

## J. Whole agreement

136. The parties acknowledge that these Terms must be read with Attvest's Privacy Policy, code of conduct, terms and conditions and other specific contracts between the user and Attvest (as applicable and which may supplement, amend or supersede these Terms or part thereof), which together comprise the whole of the agreement between the parties with respect to the use of Attvest's InfoTech, including ATTtransact, and any representations or warranties made or implied or expected by any party prior to your acceptance of these Terms will have no force or effect.



ATTVEST Pty Ltd ABN 37 169 039 221  
Brisbane Technology Park, Unit 5, 88 Brandl Street  
Eight Mile Plains, Brisbane 4113  
✉: PO Box 7055, Upper Mt Gravatt QLD 4122  
☎: 1300 363590  
@: service@attvest.com.au  
Version 1 of 2023