

For enquiries, message us on the Bankwest App or Bankwest Online Banking, or call us on 13 17 19 If you're a business customer, call 13 7000

# BUSINESS ZERO TRAN ACCOUNT STATEMENT

BSB Number 302-961

Account Number 027379-8

Period

25 May 19 - 26 Aug 19

Page 1 of 3

Statement Number 10

BS2383AN01 004086-000000 (009R)
THE DIRECTOR
OLDFIELD CAPITAL SUPERANNUATION FUND
57A NORTHCOTE STREET
AUBURN NSW 2144

Account of: OLDFIELD CAPITAL PTY LTD

Date	Particulars	Debit	Credit	Balance
25 MAY 19	OPENING BALANCE			23,130.43
27 MAY 19	ASIC Review Fee	53.00		23,077.43
19 JUN 19	ABN98002348352 ET190619CTR0656B81		537.59	23,615.02
24 JUL 19	ABN98002348352 ET190724CTR0651D8D		12.29	
24 JUL 19	ABN98002348352 ET190724CTR0651F29		428.00	24,055.31
20 AUG 19	ABN98002348352 ET190820CTR0658DFC		434.43	24,489.74
26 AUG 19	CLOSING BALANCE			24,489.74
	TOTAL DEBITS	\$53.00		
	TOTAL CREDI	rs	\$1,412.31	

BS2383AN01 / 004086 / 0006489

Make sure you check the entries on this statement carefully. If you see something that doesn't seem right, call us on 13 17 19. For more info about your account or disputing transactions, see the relevant Product Disclosure Statement – it's available on our website, at your local Bankwest branch or by calling us on 13 17 19. If you don't want to receive promotional info from us, let us know by calling 13 17 19.

# IMPORTANT NOTICE PROTECTING YOUR ACCESS METHODS

Your Bankwest Card, Mobile Device, Mobile Wallet, Payment Device, Biometric Identifier, Security Token, Personal Identification Number (PIN) and Security Code are the keys to accessing your accounts electronically. As a result, ensuring they are safe and secure from unauthorised use at all times, is very important. In these guidelines, we refer to your PIN and Security Code as your "Secret Code" while "card" refers to credit cards and debit cards.

### Protecting your card

To protect your card, you should:

- Sign your card as soon as you receive it;
- Carry your card with you whenever possible;
- · Keep your card in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- Never lend your card to anybody, or give the details on your card (such as the card number or expiry date) to anyone;
   Do not allow anyone to see the details on your sand when your sand when
- Do not allow anyone to see the details on your card when you enter them into a EFTPOS machine, ATM or other electronic
  equipment;
- Ensure you retrieve your card after making a transaction; and
- · Destroy your card when it expires or is no longer valid by cutting it diagonally in half.

## **Protecting your Secret Code**

To protect your Secret Code, you should:

- Memorise your Secret Code when you receive it and destroy the notice advising you of the Secret Code;
- Never disclose your Secret Code to anyone even family, friends or persons in authority (such as a bank officer or police officer);
- Be careful to prevent anyone from seeing you enter your Secret Code into an EFTPOS machine, ATM or other electronic equipment;
- Never keep a record of your Secret Code on your card, even if it is disguised;
- Never choose a Secret Code which can be easily identified with you i.e. your name, date of birth, car registration, telephone number or anything else that could be associated with you;
- Never choose a Secret Code which has an easily retrievable combination such as 1111, 1234 or ABCD;
- If you must record your Secret Code, make a reasonable attempt to disguise it. For instance, do NOT record it in reverse
  order or as a series of numbers with any of them marked to indicate the Secret Code; and,
- Do not use any forms of disguise to your Secret Code that could be easily discovered by another person.
- If you suspect someone else may know your Secret Code or that an unauthorised person is using your Secret Code, you should contact us immediately to request the issue of a new Secret Code.

#### Protecting your Mobile Wallet

To protect your Mobile Wallet, you should:

- Ensure your mobile device is locked at all times when it is not being used, and is not left unattended in a non-secure environment;
- Ensure you install and regularly update anti-virus software on the mobile device;
- · Ensure that only you access the Mobile Wallet to use your card and that it is not accessed or used by anyone else; and
- · Remove any card from your mobile device before disposing of your mobile device.

If your mobile device can be accessed by a Biometric Identifier, such as a fingerprint, you should ensure only your Biometric Identifier is registered on the mobile device.

#### Protecting your Payment Device

To protect your Payment Device, you should:

- Keep the Payment Device in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- · Do not expose the Payment Device to high heat, or attempt to dissemble it or keep it near electromagnetic fields;
- Do not keep the Payment Device with any document containing the reference numbers for nominated accounts or with other account information such as statements or cheque books; and
- Do not lend the Payment Device to anyone, or permit anyone to use the Payment Device.

#### Protecting your Biometric Identifier

If another person's Biometric Identifier, such as but not limited to a fingerprint, is loaded onto your mobile device, you must ensure you take immediate steps to remove this Biometric Identifier from your relevant mobile device, otherwise any transaction using that Biometric Identifier will not be an unauthorised transaction for the purposes of determining liability.

### Protecting your Security Token

To protect your Security Token, you should:

- · Carry the Security Token whenever possible;
- · Always keep the Security Token in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- · Do not record account numbers, PANs or Secret Code details on the Security Token;
- · Do not drop the Security Token or expose it to high heat, water or attempt to disassemble it;