



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

BSB Number	303-092
Account Number	316959-3
Period	24 Dec 21 - 23 Jun 22
Page 1 of 3	Statement Number 24

Name	PAN
SIMON JONATHAN STORM	1330454

MR S STORM
38 HAWKSTONE STREET
COTTESLOE WA 6011

Account of: SIMON JONATHAN STORM

TRANSACTION DETAILS FOR ACCOUNT NUMBER: 316959-3				
Date	Particulars	Debit	Credit	Balance
24 DEC 21	OPENING BALANCE			\$1,010.73
04 JAN 22	CREDIT INTEREST		\$0.05	\$1,010.78
01 FEB 22	CREDIT INTEREST		\$0.04	\$1,010.82
01 MAR 22	CREDIT INTEREST		\$0.04	\$1,010.86
01 APR 22	CREDIT INTEREST		\$0.04	\$1,010.90
02 MAY 22	CREDIT INTEREST		\$0.04	\$1,010.94
01 JUN 22	CREDIT INTEREST		\$0.04	\$1,010.98
23 JUN 22	CLOSING BALANCE			\$1,010.98
	TOTAL DEBITS	\$0.00		
	TOTAL CREDITS		\$0.25	
23 DEC 21	Credit Interest Rates Tier 1	\$0.00+	@	0.0500% p.a.

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 information about your account, and for details of the dispute resolution mechanism that covers disputed transactions and complaints (including how to access the mechanism and to make a complaint – including to the external dispute resolution body - the Australian Financial Complaints Authority), please see the Product Disclosure Statement for this product (available at our website and branches), or call/visit us. Bankwest, a division of Commonwealth Bank of Australia ABN 48 123 123 124 AFSL / Australian credit licence 234945. If you don't want to receive promotional information from us, let us know by calling us on 13 17 19.

You and your security – ePayments Code reminder

Why am I receiving this notice?

The ePayments Code applies to your electronic payment transactions, including ATM transactions, EFTPOS Transactions, Online Payments, BPAY payments, Internet Banking, Mobile Banking and Credit Card Transactions. As Bankwest is a member to this Code, we need to remind you about your Card, Pin and Online security. 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. Ensuring they are safe and secure from unauthorised use at all times, is very important.

We provide this notice to you as a reminder

1. To protect your cards, PIN, Secret Codes, Mobile Wallet, Payment Device, Biometric Identifier and Security Token.
2. On how to report unauthorised use, loss, and theft. Including the steps you need to take to notify us.

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 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 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;
- Do not keep the Security Token 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 Security Token to anyone, or permit anyone to use the Security Token.

Reporting unauthorised use, loss and theft

It is important you immediately contact us if you become aware of any of the following:

- Your card or Payment Device has been lost, stolen or used without your authorisation;
- Your Secret Code or Security Token has been lost, stolen or become known to or used by anyone else; or
- Your mobile device on which your card has been loaded using a Mobile Wallet has been stolen, lost or used without authorisation.

Note: These guidelines provide examples only of security measures and will not determine your liability for any losses resulting from unauthorised transactions. Liability for unauthorised transactions will be determined in accordance with the ePayments Code. For example, you will not be liable for losses arising from an unauthorised transaction in the following circumstances:

- Where the unauthorised transaction occurs before you've received your Secret Code, card, Payment Device or Security Token, or after you've alerted us of the misuse, loss or theft of the card, Payment Device, Security Token or disclosure of the Secret Code;
- Where you have not contributed to the loss;
- Where the access method was faulty; or
- Where we (or our agents) or a merchant has acted negligently or fraudulently.

However, if you have contributed to losses you may be liable – but only for those losses which occur before we are notified of the unauthorised use of a card, Payment Device, or Security Token or breach of your Secret Code. You won't be liable for losses that exceeds applicable transaction limits that apply to a relevant period, or losses greater than the balance of your account (including pre-arranged credit), or losses on accounts that you have not agreed could be accessed using the card or Secret Code.

In all other cases, your liability from an unauthorised transaction could be limited to the lesser of \$150, your account balance or the actual loss.

For further details on liability for unauthorised transactions, please see the Account Access Conditions of Use document, available on bankwest.com.au.

What to do if your statement is incorrect

Firstly, don't delay in telling us. **You should make every effort to report any transaction which you dispute within 14 days of the date of the account statement on which it appears.**

This is to help us ask for a chargeback (a reversal of the card transaction from the retailer or service provider) where we have a right to do so. Under the rules of the card scheme, Bankwest has the right to seek a chargeback by having the transaction debited to the retailer's or service provider's account with its financial institution. Not all disputed transactions will be successfully charged back. The chargeback must first be accepted by the retailer's or service provider's financial institution. There are a number of grounds on which Bankwest has the right to claim a chargeback, for instance if you tell us that a transaction has been debited to your account without your or any additional cardholder's authority.

Simply complete and submit a Bankwest Transaction Dispute Form. We will notify you of the name and contact number of the officer investigating your dispute.

Get things started

- **Message us 24/7** in the Bankwest App;
- Call us on **13 17 19**;
- Go to our website, bankwest.com.au and follow the procedures it sets out for disputing a transaction;
- Visit a Bankwest branch; or
- Write to us at the address shown on your account statement.

To help us resolve the issue quickly you will need to supply details of the transaction, including:

- Your name, address, card number and account details;
- Details and amount of the transaction, charge, refund or payment in question; and
- Supporting documentation (examples being: receipt, delivery advice).

Help us to help you

Failure to report a disputed transaction, charge, refund or payment, and/or provide additional information within 14 days of the date of the account statement could affect our ability to claim a chargeback right (if any) under the card scheme rules. These rules all impose time limits on reporting disputed transactions, charges, refunds or payments. In certain circumstances where the ePayments Code applies, there may be no such timeframes imposed upon your right to make a claim or report a disputed transaction.