



Osko

South West Slopes Credit Union will be participating in an industry wide initiative of New Payments Platform Australia that allows our members to transfer money to other financial institutions faster, simpler and smarter. Currently, this can take up to 48 hours. Osko® will allow you to electronically transfer funds in less than a minute.



Benefits of Osko:



Faster

Pay and get paid in less than a minute, 24/7.



Simpler

Pay to a mobile number and/or an email address.



Smarter

Use emojis and up to 280 characters to describe your payment.



Safe

It's backed by BPAY and us, so it's very safe and secure.

PayID – what is it?

For personal banking you can address payments to a mobile number or email address. For business' an ABN/ACN can be used.

Faster and simpler

PayID is designed to work seamlessly with the new Osko by BPAY service, which we are integrating into our Internet Banking and Mobile Banking App. You'll soon be able to make and receive payments faster than ever before, 24/7.

Pay the right person every time

If you've ever worried about sending money to the wrong person, PayID can help.

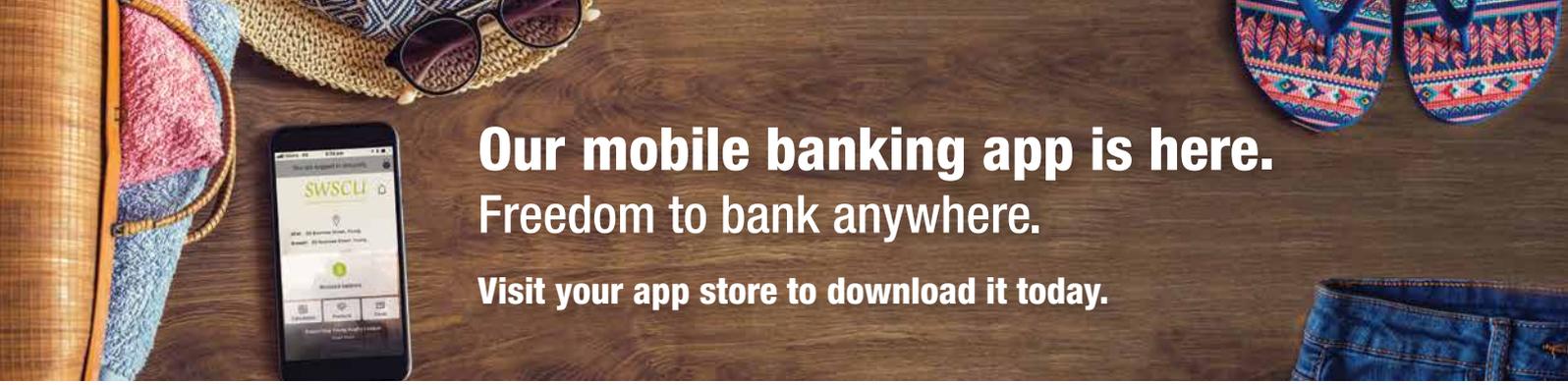
When you use a PayID to transfer money the system will automatically show you the name of the person the PayID is registered to before you send the money. So you can be confident knowing your money is going to the right place.

BSB and account numbers will still exist

PayID is an easier way to pay someone – it won't be replacing regular transfers or BPAY. You can choose not to register a PayID and continue using BSB and account numbers to pay or get paid by others (a PayID will be easier, though).

If you would like to continue using your account number for transfers but want to be part of OSKO to send and receive payments within seconds, a new BSB will need to be provided.





Our mobile banking app is here. Freedom to bank anywhere.

Visit your app store to download it today.

Identity theft

Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits.

Common examples of identity theft methods

- Phishing – the scammer tricks you into handing over your personal information.
- Hacking – the scammer gains access to your information.
- Remote access scams – the scammer tricks you into giving access to your computer.
- Malware and ransomware – the scammer installs software on your computer.
- Fake online profiles – the scammer sets up a fake profile.
- Document theft – the scammer gets access to your private information.

Warning signs

- You receive an email, text or a phone call out of the blue asking you to 'validate' or 'confirm' your personal details by clicking on a link or opening an attachment.
- There are unexpected pop-ups on your computer or mobile device.
- You receive a friend request from someone you don't know on social media.
- You are unable to log into your social media or email account.
- You notice that amounts of money go missing from your bank account.

Protect yourself

- Do not open suspicious texts or emails – delete them.
- Verify the identity of the contact – by finding them through an independent source such as a phone book or online search.
- Never send money, give credit card or online account details.
- Choose passwords that would be difficult for others to guess, and update them regularly.
- Secure your networks and devices with anti-virus software and a good firewall.
- Be very careful about how much personal information you share on social network sites.
- Put a lock on your mailbox and shred or destroy any documents containing personal information before disposing of them.
- Find out how to get a free copy of your credit report from the ASIC MoneySmart (link is external) website.



Have you been scammed?

If you think you have provided your account details, passport, tax file number, licence, Medicare or other personal identification details to a scammer contact your financial institution, or other relevant agencies immediately.

For more information visit
www.scamwatch.com.au