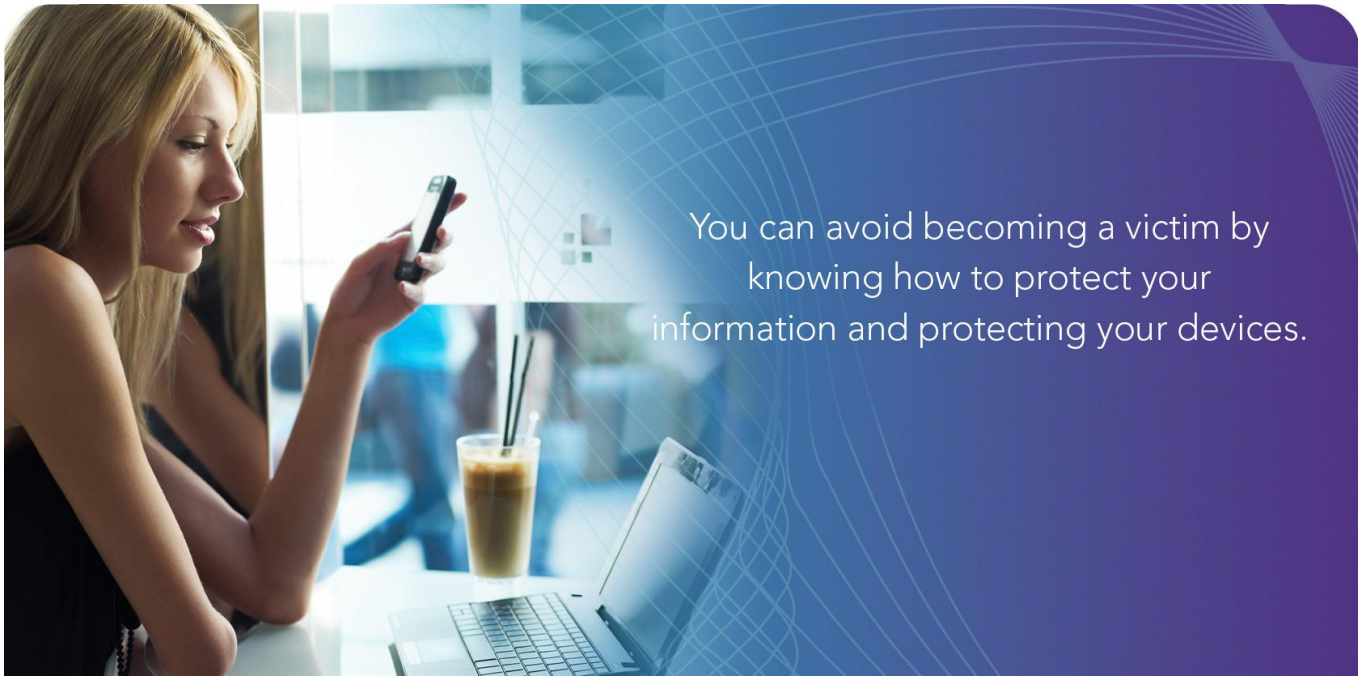
AUSTRALIAN BANKERS' ASSOCIATION INC.

Banking on the go – security tips for your smartphone and tablet

Australians love new technology. According to a global survey by Google[i], Australia has one of the highest smartphone penetrations in the world at 37 per cent – just behind Singapore – and we're also consuming more applications (apps) than the US or Britain. The research noted we're also leading the way in mobile banking, with Australians 65 per cent more likely than the British and 14 per cent more likely than Americans to conduct banking on our phones. And by 2016, mobile payments are expected to reach $US617 billion worldwide – that's nearly a sixfold increase from 2011 at $US105 billion[ii]. That's because banking on your computer, tablet or smartphone is so convenient. You can do your banking when it suits you, not just when the branch doors are open. Banking from your office, the lounge room, when travelling and on holidays – being able to do your banking whenever and wherever you like, puts you in charge. Being able to check your balances, track your savings, set goals and make payments all help you control your finances.

Unfortunately criminals see opportunities whenever money is involved – they will always seek new ways to steal and commit fraud. Banks protect your accounts with sophisticated software systems which track suspicious transactions. Criminals know it's very difficult to defeat these systems, so they focus on targeting customers directly, tricking people into revealing information that should remain confidential.

But you can avoid becoming a victim by knowing how to protect your information and your devices, including your computer, tablet or smartphone, and understanding how criminals use scams to try to defraud people. This fact sheet prepared by the Australian Bankers' Association (ABA) and the Australian Federal Police (AFP) provides some useful information and outlines some simple security steps to protect your valuable personal information.



What transactions can you do with mobile banking?

It may be possible to access your banking using your smartphone or tablet in two ways. You may be able to access Internet banking directly or your bank may have developed a mobile device app. These two services enable you to make payments on the go via e-mail, social networks, BPAY[iii] and smartphone to smartphone.

Each bank has different features on their mobile apps but below are some of the ways you can complete your banking on your smartphone or tablet (check with your bank which options it offers).

Some of the options include:

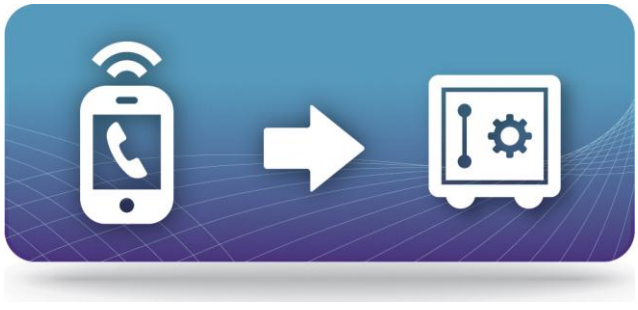
Pay a bill via BPAY

Anna has just noticed her gas bill is due in the next few days so she decides to pay by BPAY.

Because she's paid the gas company via BPAY before, the details are stored in her BPAY biller address book in her bank app or in Internet banking. That means she can pay the bill via BPAY on her mobile or tablet. Choose the BPAY icon and follow the prompts to pay the bill. She pays the bill on time, gets a receipt number for the payment and avoids overdue charges from the gas company.

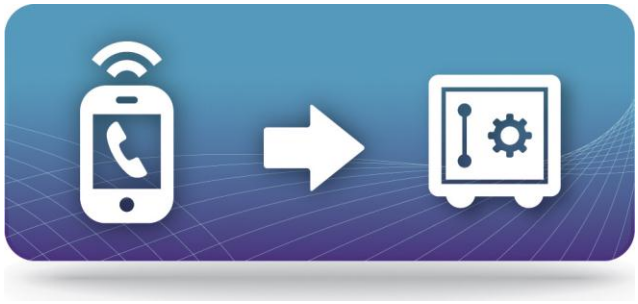
You may also be able to add billers into the mobile banking app and it may be available in Internet banking as well.

Check your balances and make transfers in between accounts at your bank



You've been saving for a new computer. Each time you get paid, you transfer $50 from your transaction account into your online savings account which attracts a competitive interest rate. You can check your balance and see your savings grow as you move closer to your goal.

Access your transaction history



At the shopping centre, you see a present that you'd like to buy for a friend. You know you've been making a lot of payments recently and want to check how much you've spent on your credit card before you make another purchase. Before you decide to buy the present, you use your smartphone or tablet to view your recent transactions and check your balance. Then you can decide whether you still want to buy the present.

Find your nearest ATM

ATMs provide convenient 24/7 access to your money when you're out.

Internet banking and your banking app may have a function to help you find the nearest ATM owned by your bank.

Bank customers should locate bank-owned ATMs because generally transactions at these ATMs are free.

Banks don't own all ATMs – many of the cash machines you see in petrol stations, convenience stores, pubs and clubs are owned by other operators.

If customers use an ATM which belongs to another financial institution or company and is not in a networked arrangement with their bank, then the customer will pay a fee charged directly by the ATM operator.

If customers use an ATM which belongs to their bank or a fee-free networked ATM, they can minimise fees.

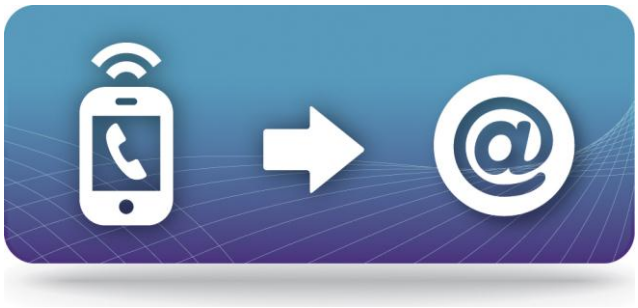
Finding an ATM that belongs to your bank or is in a networked arrangement is important if you want to avoid an ATM operator fee.

Tools and calculators

Some banks offer tools which feature on their Internet banking websites such as home loan calculators, currency converters and share trading options.

At present, not all banks offer all the following features, so check with your bank about what you can do with your banks' mobile banking app.

Pay on the go via e-mail



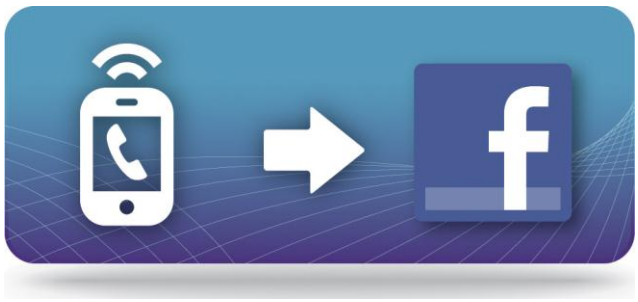
John rings and says he'll organise tickets for the football at the weekend if you'd like to go with him.

You agree and send him the money for the ticket by e-mail using your mobile banking app.

You open your app, select the pay by e-mail icon, select John's contact or enter his e-mail address, insert the amount you want to send, confirm the details and then send the payment to him.

Different banks have different ways to collect payments, so check your bank's website, listed at the end of this fact sheet for details.

Pay via Facebook friends



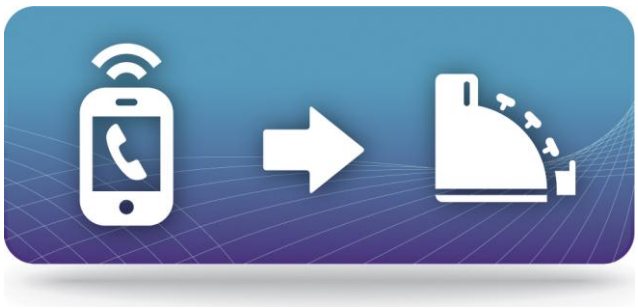
A group of your friends are all going to meet at the cinema to see a movie and to make sure you all get tickets, you decide to pre-pay.

Your friend Andy will make the group booking and pay for everyone's tickets. You then reimburse him via Facebook.

You choose the pay by Facebook icon on your mobile banking app, search by name and select Andy, then insert the amount and confirm the details.

Andy picks up the payment and it's done. Check with your bank on how to pick up a payment.

Turn your phone into a contactless payment device and use it where these payments are accepted



To use this service, Commonwealth Bank requires you to buy an 'iCarte' – a case for your phone. This enables payments to be made by waving or tapping your phone at a merchant's terminal, where these payments are accepted.

For example, you can buy a coffee and a muffin for breakfast at your local convenience store that has a contactless terminal. Once the cost of the coffee and muffin is rung up on the till, you pay by waving or tapping your phone at the terminal. It keeps you moving so you don't miss your train and you keep your cash to use later in the day.

How banks protect your money

Mobile banking is safe and secure. Banks build in strong security measures to protect your accounts:

- **banks provide PINs and passwords on accounts** which should be kept confidential;
- **lock-outs and time-outs** – for example, some apps give you five attempts to enter your PIN correctly. After that, the app is locked ensuring others can't attempt to guess your PIN. And after three minutes of inactivity, the app may log you out, in case you forget to close it;
- **monitoring** of your accounts and providing customer authentication procedures; and
- **backing of the banks' security guarantee** – banks will cover any losses if there is an unauthorised transaction on your account provided you protect your PIN and password. Customers must notify their bank if there is a loss, theft or misuse of their PIN and/or any suspicious activity on the account.

Criminals will see opportunities wherever money is handled – whether that's in cyberspace or on the street. While banks are using technology to make their products and services more convenient for you, they're also working to ensure their policies and practices are in sync with your expectations around privacy.

Banks give you a security guarantee, in the unlikely event your account is compromised by criminals. Bank customers are protected from loss in genuine fraud cases. There's usually an investigation by the

bank to determine how the fraud has occurred, but if you are an innocent victim, then the bank will cover your losses.

Banks will protect customer privacy because their future depends on it. Banks need customer trust – it's their most valuable asset. That's why the banking industry is committed to securing your confidential personal information.

Today it's commonplace for customers to complete transactions overseas – such as buying goods online from companies located in other countries. This means consumers are sending information overseas on a daily basis.

It also doesn't matter where the information is held, as Australian banks; they're obliged to meet Australian laws on privacy and security, no matter how or where banks process your information.

All retail banks are signed up to ASIC's Electronic Funds Transfer (EFT) Code which is a code of practice which sets out rules about how electronic funds transfers should work. All retail banks offering electronic banking services are signatories to the Code.

This means that banks' customers are protected – they are not liable if unauthorised transactions are made with their cards, smartphone or tablet and will be reimbursed their funds as long as they have taken due care to protect the privacy of access codes and passwords.

The Code has recently been updated and has had its name changed to the ePayments Code. It regulates electronic payments including ATM, EFTPOS, credit card transactions, online payments, Internet and mobile banking and BPAY. ASIC notes on its website that "*organisations are progressively transitioning from the old EFT Code and will all have done so by 20 March 2013."*

What do criminals target?

Criminals want to get your personal information so they can commit fraud and identity theft. It's not just Internet banking passwords and PINs which they use to defraud you. They may use personal information such as your driver's licence number, passport details or address – the combination of which can allow a criminal to assume your identity and conduct transactions in your name.

How do criminals do it?

Criminals usually try to trick you into revealing your personal information. Here are some of the more common deceptive practices:

- **Hoax messages:** e-mails, text messages or Internet pop-ups that direct you to fake websites which prompt you to reveal personal information;
- **Malware:** you may inadvertently download software that can monitor where you go online and record your keystrokes. This means that the software can record your confidential Internet banking passwords, logons, and other personal information. Criminals can then access that information to commit fraud;
- **Fake phone surveys:** Criminals claiming to be from an authorised company, contact you and ask questions designed to trick you into revealing personal information;
- **Website scams:** criminals aim to target a large number of people by running a scam, sometimes a 'too good to be true' offer on a social network website where friends and families share information; and
- **Phone porting:** criminals may switch your phone to another provider, thereby gaining access to your calls and SMS. Once the transfer is complete, they can start conducting transactions in your name. To achieve this type of fraud, criminals need confidential Internet banking logons which they may get by other means.

Examples of scams

It is useful to understand what these scams look like so that you can recognise them and avoid the traps.

Hoax messages

Criminals may send e-mails, text messages or phone you claiming to be from your bank or another legitimate organisation. These messages often ask a series of questions leading you to provide PINs or Internet banking passwords or logon details. The e-mail or text message may contain a link to a fake bank website. From here, criminals can retrieve any data that you enter.

Even though your bank will call you if they suspect there is suspicious activity occurring on your bank account or credit card, banks will never ask you to provide confidential passwords or PINs verbally, via e-mail or via a phone keypad. Should you receive requests such as these, do not respond. Check your banks' websites for further information or call your bank for advice. If you have provided any information, call your bank and staff will take immediate action to protect your account.

Example a of hoax e-mail

From: *Suncorp Bank [mailto:support@Suncorp.com]*
Sent: *Monday, 9 April 2012 11:35 AM*

To: *heather.wellard@bankers.asn.au*
Subject: *Internet Banking*

We need your help

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to your Suncorp Bank account. We want to work with you to get your account back to normal as quickly as possible.

What's the problem?

For reasons relating to the safe use of the Suncorp Bank service we need some more information about the use of your credit or debit card linked to your Suncorp Bank account.

Reference Number: PP-001-593-849-323

How you can help

It's usually quite straightforward to take care of these things. Most of the time, we just need some more information about your account or latest transactions.

To help us with this and to find out what you can and can't do with your account until the issue is resolved.

Yours sincerely,
Suncorp Bank

Suncorp Bank E-mail ID PP1589

Scams that exploit your goodwill

Criminals may also send e-mail or text messages posing as an organisation or a person that you recognise. The messages may ask for an urgent response, for example, sending money to a friend who is in trouble overseas. The convincing message will ask you to send money so they can get home. The problem is that your friend may not even be travelling and the message is from a criminal. Always contact the family member or friend through alternative means before agreeing to any request.

The criminals craft these personalised scams by gathering information via social networks and search engines, and then make a request backed by a lot of information about the person, or you, so that it appears legitimate. The scammers are probably making the same request to hundreds of people, but using personalised information. Criminals search the Internet for information and may also rob your letterbox or sift through your bin to get hold of personal documents such as bank accounts and bills.

Phone porting

Fraudsters harvest personal information and smartphone numbers to request a smartphone provider to switch or 'port' a victim's number to a new device. If you are a victim, they may send you a message to advise you that your current provider is experiencing difficulties – this buys the criminals more time.

Once your number is successfully 'ported', the criminals gain control of your calls and SMS messages. They may also obtain your Internet banking logon through other means and so receive SMS security or verification messages that allow transactions to proceed; allowing them to make unauthorised transactions in your name. The bank may identify these transactions as unusual and contact you.

Job scams

Fraudsters set up fake job ads and harvest personal information to steal identities with the aim of committing identity fraud. Or they trap people into laundering money for criminals by becoming a money mule.

The fake job ads make the opportunity sound enticing, saying things like "work from home, no experience necessary, four hours a week and big salaries." But, think before you apply because if it sounds 'too good to be true', it's probably a scam!

Money mules

A money mule is someone who allows their bank account to be used to receive stolen funds which are transferred to a designated account (domestic or offshore) using a money-remitting or wire service, minus a commission payment. The mule is usually approached online, via e-mail or instant message, or criminals may advertise on legitimate employment websites and in publications.

These scams involve people in a criminal enterprise and there are serious penalties under Australian and international laws for laundering money. The prospect of making easy money may appear attractive to the unemployed or people who are looking to earn money in their spare time such as students.

There are some serious ramifications for anyone who gets involved in a mule scam. For example, any 'commission' payments can be confiscated (as proceeds of crime) and the money mule could become the subject of a police investigation that may lead to a maximum penalty of 20 years' imprisonment. Bank customers who participate in money laundering could face prosecution, have banking facilities withdrawn and could have their identity stolen by the criminals as well.

Never provide confidential banking details to anyone and take steps to verify the background of any company or person that makes you a job offer.

If you would like to read more, the ABA has another fact sheet with useful tips on how to avoid these scams including being cautious about accepting job opportunities that offer anyone the chance of making money simply by moving money in and out of any bank account.

The fact sheet is called *"Money Mules Explained"* and can be accessed from the ABA website: http://www.bankers.asn.au/Consumers/Security-and-Fraud-Prevention

Social networking hints – play it safe

Popular websites and forums, such as social network websites are places where criminals can harvest information about people. These websites encourage information sharing and allow you to connect with a wide range of people regardless of their location. When you are on a website that encourages open communication, it can be easy to let down your guard and provide confidential or personal information that should remain private.

Hints

- **Be careful what you post online** – don't give out too much information about yourself. For example, do not include phone numbers, addresses, your birth date or other personal information which could be used to steal your identity.
- **When adding friends to your network, be careful whom you choose to accept.** The new 'friend' who is outside your social circle may be a criminal looking to gain information about you.
- **Check the privacy and security settings** of the social networking website. You may wish to adjust the default settings which usually let people have more access than you may wish.
- **Read the privacy policy** of the social network website carefully so that you understand how the organisation may use the information that you post online.

Security tips

Online browsing can unwittingly expose you to malware or viruses which infect your computer or mobile device and make your information available to criminals. There are some good practices and some simple actions that may reduce the likelihood that information will be compromised.

- **Lock** – set your smartphone and tablet to automatically lock. The password will protect your device so that no-one else can use or view your information. Also store your device in a secure location.
- **Contact your bank if you lose your smartphone or tablet** – call your bank immediately to tell staff about the loss and provide your new mobile number especially if your bank uses an SMS message to authenticate transactions.
- **Clear your mobile device** of text messages from banks especially before sharing, discarding or selling your device.
- **Be careful what you send via text** – never use text messages to disclose any personal information, such as account numbers, passwords or other personal information which could be used to steal your identity.
- **Use only official apps** – make sure to only use apps supplied by your financial institution and only download them from official app stores.
- **Protect your tablet and smartphone** – install and keep up-to-date anti-virus and firewall software purchased from trusted suppliers. It is important to update the software because new viruses emerge for which software providers create new barriers to deal with the new threats.
- **Protect your passwords** – ensure you keep confidential your PIN and Internet banking logons and passwords. Avoid using the same login passwords for multiple websites, especially when it enables access to websites that include sensitive personal information. Set a pass code for your device and a PIN for your SIM. If your banking app allows login with a PIN, make sure it is different to the one used to unlock your mobile device. Make sure your password or code is something that's hard for others to guess but easy for you to remember.
- **Read privacy policies** – before you provide personal information to any website, understand how your information will be used and how long it will be retained.

- **Be wary of free downloads, programs, software or screensavers** – sometimes malware and spyware can be hidden in free offers of other files.
- **Beware of hoax e-mails** – be alert to offers that are 'too good to be true' or are designed to elicit an emotional response and triggers the thought of sending money. Always question messages that come out of the blue and verify the authenticity through trusted channels. Do not respond using information or links provided in the original message. No bank will ever send customers an e-mail with a link to online banking or ask for confidential information, so treat with suspicion any unsolicited e-mail that appears to be from your bank.
- **Check your bank account statements** – urgently contact your bank immediately if you find any unusual or suspicious transactions. Your bank will then take action to protect your account. Bank staff may call you before your statement has arrived to advise you of unusual activity on your account.
- **Don't store your banking PINs or passwords in your smartphone or tablet** – this makes your account vulnerable if the device is lost or stolen.
- **Regularly clear your browser's cache** – some mobile devices store copies of web pages that may contain your banking information.
- **Always log out** of Internet banking sessions once you've finished.
- **Be aware** – when using Internet banking in busy, public areas, check for people looking over your shoulder.
- **Wi-Fi** – don't conduct Internet banking using unsecured Wi-Fi networks.
- **Device security** – don't conduct Internet banking transactions on a jailbroken device. A jailbroken device is any electronic device not designed or authorised by the parent company.

Read more about banks' mobile banking apps

ANZ: http://www.anz.com/personal/ways-bank/mobile-banking/banking-iphone/

Bank of Queensland: http://www.boq.com.au/online_IB_faq_mobilebanking.htm

Beirut Hellenic Bank: http://www.beiruthellenic.com.au/MobileBanking

Bendigo and Adelaide Bank: http://www.bendigobank.com.au/public/e-banking/faq.asp?zoom_highlight=mobile

Citigroup: http://www.citibank.com.au/aus/banking/banking_internetbanking.htm#CitibankMobile

Commonwealth Bank: http://www.commbank.com.au/personal/netbank/netbank-for-mobile/

BankWest: http://www.bankwest.com.au/personal/payments-services/ways-to-bank-with-us/mobile-banking

HSBC: http://www.hsbc.com.au/1/2/personal/services/mobile-banking#top

ING Direct: http://www.ingdirect.com.au/mobile

Macquarie Bank: http://www.macquarie.com.au/mgl/au/advisers/keep-up-to-date/news/access-mobile

National Australia Bank:
http://www.nab.com.au/wps/wcm/connect/nab/nab/home/personal_finance/12/40/1?S_KWCID=SEADW

Suncorp: http://www.suncorpbank.com.au/iphone-android-app

United Overseas Bank:
http://www.uob.com.sg/personal/ebanking/mobile/index.html?s_pid=HOME201205_eg_mbk_dlapppbtn

Westpac: http://www.westpac.com.au/personal-banking/mobile-banking

Document Created: September 2012

Any other questions?

Please contact ABA Director Public Relations Heather Wellard on 02 8298 0411, e-mail **Heather Wellard** or write to the ABA at Level 3, 56 Pitt Street, Sydney, NSW 2000.

Internet: **www.bankers.asn.au**
Twitter: @austbankers

Ph: 02 8298 0417
Fax: 02 8298 0402

Proudly supported by the

AUSTRALIAN FEDERAL POLICE

---

[i] Smartphone surge challenging the PC by Nic Christensen, The Australian, September 09, 2011
http://www.theaustralian.com.au/australian-it/smartphone-surge-challenging-the-pc/story-e6frgakx-1226132628041

[ii] According to research by Gartner referred to in "Cashing in on demand for the digital wallet" by David Sarno, "The Australian Financial Review", page 30, July 10, 2012, originally published in "The Los Angeles Times"
http://www.afr.com/p/technology/apps_turn_smartphones_into_digital_R5kOx31EkHzQvWJxP8nCRO

[iii] You need to be registered to make a BPAY payment and that can be done by contacting your bank.