SMART Cards

A smart card, similar in size to a standard credit card, contains an embedded computer microchip, which can be programmed to perform multiple functions. The card has its own operating system, temporary memory and file storage capacity. In essence, it is like having a personal computer and bank in one's wallet or purse - without the screen or the keyboard or the cash.

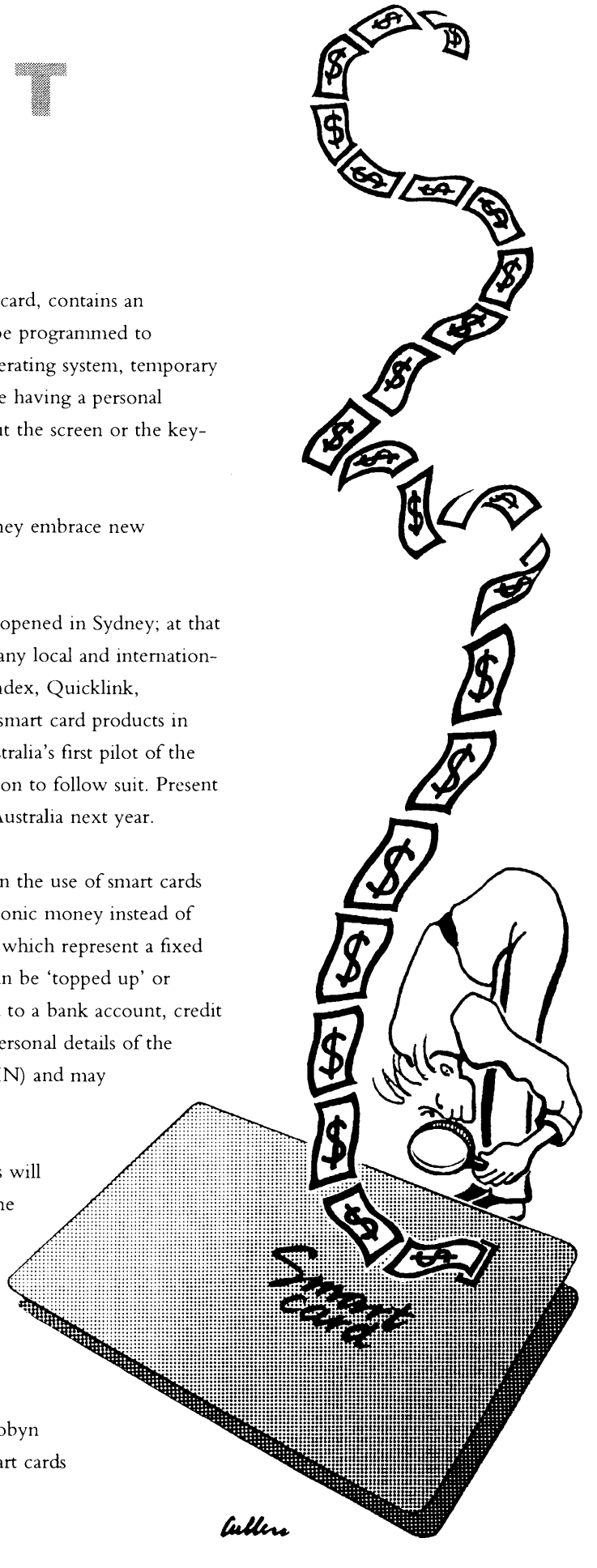
Australians are notorious for the speed with which they embrace new technology.

In 1995, Australia's first smart card production plant opened in Sydney; at that time it was one of only eight plants in the world. Many local and international smart card promoters - including Mastercard, Mondex, Quicklink, Transcard and Visa - have run test projects for their smart card products in Australia. In August this year, Westpac launched Australia's first pilot of the Mondex smart card. ANZ and NAB are expected soon to follow suit. Present predictions are that smart cards will be launched in Australia next year.

The systems trialled in Australia have concentrated on the use of smart cards as stored value cards (SVCs). These cards carry electronic money instead of cash. SVCs include the anonymous disposable cards, which represent a fixed amount of electronic money; reloadable cards that can be 'topped up' or replenished; and personalised reloadable cards, linked to a bank account, credit card account or overdraft. These cards can include personal details of the card holder, and a personal identification number (PIN) and may include biometric security features.

It is likely that within the next few years, smart cards will be multifunctional, housing such applications as airline ticketing, loyalty programs, bank debit and credit facilities, foreign currency, telephone use and telephone banking, and health records.

Here, two writers discuss different aspects of smart cards. Chris Connolly, of the Electronic Money Information Centre explores privacy issues, while Robyn Gray, of the NSW DPP, considers the impact of smart cards on law enforcement.



Big Brother's little helpers

New technologies often create or exacerbate legal problems - smart cards are no exception. Two leading applications of smart cards are their use as stored value cards (often promoted as the key to the development of the cashless society) and as health record cards. Chris Connolly* says both of these applications have the potential to seriously threaten the privacy of card users.

The stored value card (SVC) is already on trial in a number of Australian locations, and is usually promoted as a convenient replacement for cash. On closer inspection, however, there are many differences between cash and smart cards. The greatest difference is the level of anonymity that each provides for consumers, and it is this issue that has dominated legal discussions about smart cards to date.
Smart cards were first patented by Roland Moreno in 1975, but have not been widely used until now. The cost of producing the tiny computer chips has finally fallen to a level where card systems can be financially viable and Australia even has its own smart card factory. But privacy and security issues continue to hold back further development and both industry and consumers have shown a strong interest in finding solutions.

It was Moreno who first noted the potential for smart cards to have an impact on privacy. In 1975 he said that "smart cards have the potential to act as Big Brother's little helpers". He recognised that smart cards are capable of collecting greater amounts of detailed transaction information than any other method of payment. For the first time, electronic records will be created and kept of all the small purchases, movements and habits of an individual.

The ability to remain anonymous in transactions (usually by using cash) is still one of the best methods to protect personal privacy, but with the advent of smart cards, Australia may have to look to improved privacy legislation and further industry regulation for protection.

There are three broad types of SVCs, each offering a different degree of privacy protection. Firstly, there are simple disposable cards, which usually have a low value (say $50) and no identification. These cards are, however, 'accountable' in that an electronic record is kept of card use, linked to the card number.

The second type is the reloadable card, where the value can be topped up by the user, rather than throwing the card away. These cards also carry no identification, but can be linked to an individual by comparison of bank records, if the card is reloaded at a bank, automatic teller machine (ATM) or electronic funds transfer point of sale (EFTPOS) outlet. The third type is the personalised card, which does carry identification information. These cards leave a complete identified electronic trail.

Unfortunately, smart card privacy issues are confused by the introduction of a particular type of card known as Mondex (a brand of smart cards that originally developed in the UK, but is now owned by Mastercard). Mondex does not keep full transaction histories, either on the card or in a central database. Mondex originally described their cards as 'anonymous', but changed their description to 'semi-anonymous' after it was pointed out that merchants kept limited records of card use, and that the card itself recorded the last 10 transactions.

These variations make it difficult for consumers to know exactly how much information is collected about them in a smart card system. Australia's fair trading laws may be tested when smart card systems are eventually rolled out - especially if any of the smart card promoters attempt to describe their cards as 'anonymous' or 'like cash'.

Health smart cards

Health smart cards, on the other hand, have not yet been subject to a trial in Australia. Again, there are three broad types of health smart cards under development. The first type will simply store emergency medical information to be accessed by emergency personnel and treating staff. The second type will store an up-to-date version of an individual's complete medical history. The third type stores health insurance information.

The design of smart cards is such that all three of these functions could be combined on one card. They can even sit alongside other functions such as stored value, transport tokens and drivers' licences.

The most sophisticated trial of health smart cards is currently taking place in Canada in the Rimouski region of Quebec. About 7000 cards have been issued, each with five types of health information stored in the card's chip:

- identification information, including name, date of birth, health insurance number, expiry date and hospital file number;
- emergency information, including blood group, allergies, visual aids, hearing aids and the date of the last tetanus shot.
- vaccination information, including a full list of all vaccinations received;
- medication information, including both prescription and regular non-prescription drug history;
- medical care information, including a complete 'cradle to grave' medical record and family history.

This Canadian health smart card system does not include the development of a back up or 'mirror' health records database. Therefore, if an individual card is lost, the information must be re-created from scratch. Most proposed systems include a 'mirror' database to avoid this problem. Privacy concerns and costs have dogged the development of such systems, and their development has been surrounded by controversy, especially in the United States.

Medical records are considered to contain highly sensitive information. Often it is information that a patient would only feel comfortable sharing with their GP or treating doctor, and not with the wider medical community or the government. Some practitioners fear that patients will not be forthcoming with information about their illness (or their family history) if the information will then be stored on a card.

Patients may expect greater access to and control over their medical records if they are going to be stored on a card and carried on their person. Access to medical records is already a thorny issue in Australia and the law remains unclear on what circumstances must exist before a patient can view (and perhaps challenge the accuracy of) their own records. Indeed, we may see a situation emerge where the legal right to access medical information differs depending on the jurisdiction - the ACT government has indicated that it will introduce privacy legislation specific to medical records.

There is also a major fear with all card-based identification systems that function creep may result in further infringements on privacy and other freedoms. In Australia we do not have a national identification card. Medicare cards are issued one per family and are often left at home in a drawer. It would be a major change to move to a system where people have to carry an individual smart card with them at all times in order to give themselves the best chance in an emergency. Many other countries (including, ironically, Canada) have introduced a card for one purpose, which, over the years, has turned into a vital system of identification, ruling every aspect of citizens' lives.

It should be remembered that smart card systems are not cheap. Card readers would need to be installed at every point of contact between medical staff and patients, including ambulances. Smart cards themselves are expensive, unless purchased in huge quantities. In many commercial applications, customers must purchase the smart card itself for between $10 and $30 before they can use it.

Smart cards are often described as a technology searching for an application, and in the health industry this appears to be true. Smart cards remain an expensive technology, strongly associated with privacy intrusive identification cards. At a time of growing concern over the sensitive nature of medical records, it might be expected that the health industry will move towards increasing security and limiting access, rather than distributing medical records to individuals on smart cards.

The future

Australia has shown its ability to lead the way in the development of smart card technology. It may also be able to lead the way in the development of appropriate regulation. The Asia Pacific Smart Card Forum, based in Canberra, has developed a Smart Card Industry Code of Conduct that is the first of its kind in the world. The code makes extensive provisions for the protection of personal information and includes sanctions procedures for businesses who fail to comply.

The code is expected to be released before the end of 1997 and although compliance will initially be voluntary, it is a promising start for a fledgling industry, and sends a clear message that the businesses involved have listened to consumer concerns. However, it will be necessary to back up this code with legislation as the development of smart card systems becomes more widespread, and Australia must consider joining other developing nations in passing legislation to protect personal information in both the public sector and private sector.

* *Chris Connolly is the Director of the Electronic Money Information Centre.*

He can be contacted at Chrisc@socialchange.net.au

Smart Cards and the Criminal Justice System: fantastic plastic or consequences drastic?

Robyn Gray* examines the ramifications of smart card technology on the criminal justice system, particularly in the areas of theft, fraud and related offences; money laundering and tax evasion; security applications; and enhanced surveillance and audit capacity.

Theft and fraud

Smart cards are promoted as a replacement for cash. If the cards prove to be as popular as their promoters predict, both merchants and consumers will be handling cash less frequently and probably in smaller amounts than is currently the case. An obviously desired outcome from a criminal justice perspective is a reduction in the incidence and seriousness of offences relating to the theft of cash. Armed robberies will be less lucrative and the opportunities to commit them less readily available. One would expect that their incidence will decrease, as will the offences of violence usually associated with them. However, since most businesses will still need to carry a certain amount of cash, armed robberies and the like can never be eliminated.

For consumers, there is an upside and a downside in the theft 'stakes'. Consumers should benefit from any reduction in the incidence of armed robberies and related offences and, as consumers should have less need to carry cash and to physically access automatic teller machines (ATMs), because the technology allows you to reload your card via special phones, the incidence of offences (theft and fraud) at ATMs should decrease. Personal security may be enhanced.

However, for consumers the impact of theft of a smart card will, potentially, be greater than the impact of loss

of cash. If the card is of the anonymous disposable variety, the consumer will lose the balance of the stored value of the card - whatever that may be - and law enforcement authorities will have little prospect of detecting a stolen card of this type.

The consequences of theft of the more sophisticated smart cards (those with PINs or biometric security features) are potentially much more serious and will depend upon the ability of the thief to access the card.

Conventional cards have proved fairly easy to counterfeit. Smart card promoters claim that the more sophisticated variety of card is a great deal more secure than the conventional magnetic stripe credit card.

The card promoters point to the difficulty of counterfeiting or replicating the microchip embedded in the card; this is said to require a series of complicated steps for which skilled resources, large sums of money (one source estimates it as a million pounds) and access to silicon are prerequisites. The smart card can also include security devices such as encryption of communications between the smart card and the reader, PINs and biometric security features. The latter use a unique identifying human features to link the holder to the card. Examples include hand geometry, thumbprint, fingerscans, retinal patterns, voice identification and photo imagery.

If the confidence of the promoters in the security features of smart cards proves justified, their increased use will result in a reduction in the incidence of credit card fraud, with major associated benefits for financial institutions, their shareholders, consumers and all of the agencies in the criminal justice system, not least those involved in fraud investigation and prosecution.

The French experience lends some support to the confidence expressed by the promoters. According to Datamonitor, a UK based research group, bank card fraud fell by 36% in France between 1991 and 1993. In 1993, about 70% of debit cards and nearly all ATM cards in France were made with smart card technology. In other European countries, where smart card usage was much lower, fraud losses increased in the same period.

However, commonsense and experience teach us that no system is 100% secure. A 1996 report by Bell Communications Research highlighted a potential flaw, which might permit an unauthorised user to manipulate the chips contained in the card to add value to a legitimate card without appropriate authorisation. The US Smart Card Forum and other industry groups responded immediately with assurances that their system included multiple levels of security and that roll-out plans for smart cards would not be delayed.

Given the resources available to organised crime, and the potential rewards to be reaped by those who 'crack' the smart card technology, it is only a matter of time before ways are found to manipulate the chip. (It is reported that organised crime groups in Japan already have a smart card reader.) Should the technology be compromised, the potential consequences for card holders are drastic.

As many cards will be reloadable from a bank account or overdraft facility, a person with unauthorised access to a smart card could theoretically recharge it until all funds in the account or facility are exhausted. As some cards will offer the facility of downloading from an account via instructions given from a special telephone, defrauding of large amounts of money could occur very quickly - before the card holder became aware of the loss of the card.

Money laundering/ tax evasion

Law enforcement agencies are justifiably concerned that the more sophisticated smart card systems offer significantly increased opportunities for money laundering and tax evasion.

Smart cards that offer facilities such as stored value, debit/credit, foreign currency and PIN security, also may offer a small customer 'wallet', into and out of which value from a card may be transferred. This allows for safekeeping of some electronic value at home. It is possible to transfer funds between numerous smart cards and accounts over the telephone or by using a 'wallet'.

Once funds are represented by the stored value on the card, it is possible to spend the money anonymously, without reference to a bank or clearing house in Australia, and without creating an audit trail.

At present, consumers worldwide use their credit cards to spend between $625 million and $1.25 billion each year on Internet purchases. Early in the 21st Century about 550 million of us are expected to be using the Internet for this purpose.

It comes as no surprise, therefore, that law enforcement agencies are concerned about the capacity of the smart card technology to be used for anonymous payments on the Internet. Electronic money (E-money) is a smart card based system, which can be traded on the Internet without relying on credit card numbers. A company (not necessarily a bank or financial institution) issues money in the form of an electronic series of encoded digits. This can be sent to other users on the Internet in a secure format and downloaded onto a stored value card. E-money can then be used to purchase any product or service. The issues raised by E-money include the integrity of the currency issuers, the security of the technology and the vast scope for laundering it provides.

For criminals, smart cards and E-money represent an opportunity to introduce 'black money' into legitimate repositories far more quickly, simply and securely than is presently the case. The greater the number of layers through which funds pass, the more difficult it is to determine beneficial ownership and source. Electronic currency and smart cards facilitate international transfers many times on any given day. The systems also permit the reinjection of the funds into the legitimate economy without reference to banks or clearing houses.

There is an obvious tension between the desire of law enforcement agencies for accountability and an audit trail and the legitimate privacy concerns of consumers. The needs of law enforcement are only one factor that should be taken into account when considering the ultimate form of the electronic payments system. However, there are obviously legitimate causes for concern; and questions that regulators such as the US Treasury's Financial Crimes Enforcement Network (FinCEN) are asking include:

- Do the systems create and maintain an audit trail?
- Does the trail extend beyond the initial transaction to subsequent transactions in the chain?
- Will the systems be restricted to transactions below a certain amount of money, ie a cap?
- Will the systems permit effective and timely monitoring of suspicious transactions, such as repeated multiple transactions designed to evade the caps? (Can you 'smurf' the net?)
- Do the systems permit self-contained, person to person transactions without the involvement of a financial institution or other regulatory body?

Security applications

Systems utilising smart card technology will increasingly be used to improve security of access to buildings, facilities and computer networks, in both the public and private sectors. Improved security should reduce fraud, theft and related offences, with obvious benefits for law enforcement agencies and all other players in the criminal justice system.

Such technology is already in use in five maximum security prisons in New South Wales to control visitor access. The system being used combines a visitor's photographic image and a thumbprint; the cards can store a picture on what is apparently a blank surface containing only fuzzy random lines, making it difficult to forge or tamper with. In NSW, smart cards are also used to enable prisoners to operate specialised telephones. This removes the need for the presence of a custodial officer, since the list of permissible calls and the time span allowed is controlled by the smart card.

Possible future uses of smart card technology in prisons include the linking of prisoner purchases to prisoner funds via the card, storage of the prisoner's image or personal details, controlling access to various parts of the correctional centre and tracking of custodial officers in conjunction with radio duress alarms, to allow for speedy response in the event of disturbances or assault.

Increased use of smart card systems to control public access to buildings such as hospitals, airport terminals and sporting facilities is likely. At the Atlanta Olympic Games the system was used to restrict access to certain events to season ticket holders; the access gates were equipped with turnstiles that contained smart card readers and fingerprint capture devices. Use of a similar system at the Sydney Olympics has been proposed.

The federal government has trialled an adaptation of the smart card technology for prisoners released conditionally from custodial sentences, as it can be used to monitor a person's movements. In more advanced systems, the smart card, when carried, also triggers responses from detector devices and locates personnel in the premises in which they are operating. This will enable employers with highly sensitive products or information to specify different levels of access for different staff within the organisation.

A potential future novel application that has been mooted is the tagging of babies in maternity wards, ie the issuing of a smart card that produces a digital photograph of the child. This would be able to be read by the smart card reader whenever the babies were moved from the area in which they were normally expected to be. This could be used as a deterrent to child abduction.

Although the smart card has been used in France, Germany and Canada to store medical information relating to its holder, there is no current proposal for such an application in Australia. Some years ago, the Warren Centre unsuccessfully proposed the introduction of a prescription card as an antidote to fraud on the Pharmaceutical Benefits Scheme.

In Mexico, social security benefits are issued in smart card form rather than by cheques or cash. This obviously reduces the potential for theft and fraud. In Australia, a proposal pursuant to which a government issued card (initially magnetic stripe) could be used at automatic teller machines to access social security payments is under consideration. This would eliminate the need to issue cheques. Ultimately, the government issued card might be reissued as a smart card. However, given the community opposition to the Australia Card, this must be adjudged a fairly remote possibility at this stage.

Enhanced surveillance capacity

The microchip in the smart card has 100 times the storage capacity of a conventional credit card. A standard card will be capable of storing over 100 pages of information about an individual and/or their transactions. While cards currently being trialled offer only a limited number of functions, it is possible to dramatically expand the functions without incurring significant additional expense. One would expect that, given our propensity to adopt new technology, we will quickly embrace the use of smart cards for a variety of everyday transactions, from the purchase of small goods and services (both locally and on the Internet), to telephone calls, public transport, bridge tolls and taxis, as well as in telephone banking and to access debit/credit facilities.

...given our propensity to adopt new technology, we will quickly embrace the use of smart cards for a variety of everyday transactions...

Eventually, I imagine, the cards will also be used to store our personal information - travel itineraries, prescription histories, medical records, social security payments, licence and passport details and so on.

Many law enforcement agencies possess statutory powers pursuant to which they will be able to compel production to them of the records held by the smart card issuer, the smart card holder and the retailers/service providers with whom the card holder has dealt. In instances where this information has been 'delinked' or encrypted, these agencies will also be able to compel production of the records which link the name and personal details of the card holder to the relevant transactions.

The result is that law enforcement agencies will be able to compile more comprehensive and detailed profiles on suspects and targets than ever before. These profiles could contain a detailed picture of a person's movements and activities and their assets and liabilities over a lengthy period. Such information would be a very powerful investigatory tool and would provide valuable information for confiscation investigation and litigation, and any other investigation where an individual's spending patterns and capacity (as contrasted with legitimate sources of income) or movements or whereabouts at a particular time are of significance.

Government agencies such as the Australian Taxation Office (ATO) and the Department of Social Security (DSS) (and any other agency responsible for public funds) will no doubt also use their statutory powers to acquire records relating to smart card use to enhance their ability to carry out their functions under their legislation. The type of information available from smart card issuers and holders will be invaluable to the ATO in performing its audit function. Similarly, the DSS could be expected to use the information to verify the accuracy of information provided to it by those applying for or applying to continue receipt of social security benefits.

In the same vein, in any criminal proceedings in which a person's income, expenditure, spending patterns, movement or whereabouts was in issue, it would be open to the Crown or the defence to subpoena records relating to an individual's smart card to obtain further information about those issues. (The same observation applies to civil litigation, particularly family law proceedings and employment law proceedings, where such issues often arise.)

Smart cards could also be used in conjunction with conventional tracking systems to provide real-time surveillance capacity. For example, if a smart card allowing on-line transactions were used to pay for a taxi fare, and the taxi was one in which a tracking system was located, it would be possible for law enforcement agencies to locate an individual and track his or her movements while he or she was in that taxi. (For those experiencing a sudden bout of paranoia, it should be mentioned that most smart cards operate off-line.)

Conclusion

When the smart card was first patented over 20 years ago, even its inventor recognised its harmful potential: in the wrong hands, he predicted, smart cards could become "Big Brother's little helpers". It goes almost without saying that the potential for invasion of personal privacy inherent in this kind of system is huge. This has been the subject of a great deal of literature and is a concern shared by many. The applications for smart cards will need to accommodate these concerns and balance in each case the undoubted benefits of such technology against its social cost.

There will be consequences for the criminal law; we must keep in mind that however smart a card is, a clever and resourceful criminal can be smarter.

* *Robyn Gray, Deputy Solicitor (Legal), New South Wales Office of the Director of Public Prosecutions.*

The author wishes to acknowledge the assistance of Edwina Cowdery, formerly a member of the ODPP Research Unit, and her Executive Assistant, Jackie Eastburn.

Smart card web sites

Monash University Centre for Electronic Commerce:
http://www-cec.buseco.monash.edu.au/

USA: Consumer Electronic Money Task Force:
http://www.ustreas.gov:808/treasury/txtonly.html

BankSmart: An Australian commercial information site:
http://www.banksmart.com.au/