Electronic money in Australia

Mark Sneddon (*)

Introduction

Australians have enthusiastically embraced electronic banking in the form of ATMs and EFTPOS terminals and, more recently, telephone banking and bill payments. Despite its relatively small population (18 million), at the end of 1993, Australia ranked fifth among twelve major developed nations in the number of ATMs per head of population and seventh in the number of EFTPOS terminals per head of population. On each business day in 1994-1995 bank-issued EFT transaction cards were used to make 1.5 million cash withdrawals and cash advances totalling $195 million and 1.7 million purchases totalling $125 million. Purchases using transaction cards (credit or debit) issued by all financial institutions accounted for almost one-third of the value of retail trade.

These trends have encouraged the promoters of three new types of electronic payment system which are being developed in Australia currently. The first is the prepaid or stored value card (SVC) where an electronic record of a prepaid balance is maintained on a microchip on the card. The second is remote account access banking via the Internet. The third is digital money for transfer over telecommunications lines or computer networks..

Each of these systems raises novel legal and regulatory issues with which the finance industry, lawyers and government are currently coming to grips.

Stored Value Smart Cards

A smart card is a plastic card with an embedded micro-processor chip which is capable of storing significant amounts of data and performing basic computing operations. The large memory capacity means that stored data can be encrypted and better protected than on a magnetic stripe card. Because smart cards contain secure encrypted records and can do basic computing, they can operate at terminals which are offline from host computers and obtain authorisation for account transactions from the balance records in the card itself rather than having to confirm details with host computer account records.

The principal financial application of smart cards is as stored-value cards (SVCs) (or pre-paid cards) which can be used to make payments at terminals off-line. Cards are issued with pre-loaded electronic value in exchange for cash or an account debit and that value can be spent at terminals in many locations for a large number of purposes. Some card schemes provide for reloading of value at specialised terminals, ATMs, EFTPOS terminals and over specially equipped telephones.

During a purchase or funds transfer transaction, the balance on the card's chip is reduced and the balance on the receiving chip (in the merchant's terminal or receiving card) is increased. A cardholder or merchant can transfer the electronic value to its financial institution and convert it into "real" value. The initial intention is for SVCs to replace cash for small-ticket sales such as groceries, newspapers, vending machines, public transport, taxis, road tolls, take away food, movies and convenience stores.

Currently there are four trials of SVCs occurring in Australia. In New South Wales there are two card schemes - Transcard and Quicklink - based initially on a public transport fare application which have extended out to cover payments to other merchants such as parking, fast food and convenience stores. Both cards are reloadable. Visa and Mastercard are trialing general purpose SVCs. Visa has been running a trial of its disposable Visa cash card in Queensland for some months in which it has sold 50,000 cards and processed 1 million transactions.

Mastercard is running a trial of Mastercard Cash in Canberra. This is a reloadable SVC offered to existing account holders of participating banks. The chip is included on the same magnetic stripe card customers use for ATM and EFTPOS transactions. A small envelope for the card is provided which can display the balance of value on the chip.

The Visa and Mastercard SVCs require financial system intermediation for all transactions. Thus only customer to merchant or customer to financial institution transactions are permitted. No peer to peer facility is available. A full audit trail of transactions is kept, making independent reconstruction of transaction history and card balance possible (eg in case the card is damaged and unreadable or lost or stolen). The audit trail enhances accountability, fraud detection and assists law enforcement but it potentially compromises the privacy of transactions if the cardholder's identity can be linked to the chip identity. Transaction data could be sold for marketing or other purposes.

The four main Australian banks have also purchased a franchise to distribute the Mondex SVC in Australia and trials are expected of this in 1997. The Mondex card permits:

> person to person transfers of value using a pocket card-reading wallet
>
> transfers of value through telephones and personal computer terminals equipped with card readers, both peer to peer and customer to merchant or financial institution, effectively turning those telephones and computers into ATMs that dispense not physical cash but electronic value onto the card and
>
> a multi-currency option allowing for the storage of electronic value denominated in up to five different currencies on the card.

Because of its peer to peer functionality Mondex cannot offer a fully accounted system. A card's chip records the last ten transactions and a merchant chip records the day's transactions but there is no central data base of all transactions. This makes it more difficult to independently reconstruct card balance or transaction history and more difficult for law enforcement to trace Mondex transactions. However the privacy of the cardholder's transactions is correspondingly increased.

Several organisations are working on applications in which a smart card reader is attached to a personal computer or a television set or the home telephone to allow for interactive payments through the television,

the telephone or over the Internet, or deposit and withdrawal transactions with financial institutions by these means.

Legal and Regulatory Issues of SVCs

There are a multitude of such issues, most of which have not yet been resolved. Some of these include:

Regulatory Controls on Issuers of SVCs

Should issuers of SVCs be restricted to already-licensed financial institutions? Transport companies and telecommunications carriers which have an existing population of card holders don't think so. Yet consumer groups and the central bank are rightly concerned with the risk of insolvency of the issuer making all the holders of electronic claims unsecured creditors. It seems likely that all issuers, whether or not regulated financial institutions will be subject to some prudential regulation. This, and the wider issue of disintermediation of regulated financial institutions out of the payments system, are before the federal government's Financial System Inquiry (Wallis Inquiry) at the moment.

Consumer Protection Issues

These include:

the application of current consumer protection codes and laws

loss allocation in the event of

card or system malfunction including ascertainment and recovery of unused balanc

alleged unauthorised transactions following loss or theft of card.

The Australian EFT code of Conduct covers ATM and EFTPOS transactions. It does not cover SVC transactions unless they involve upload or download to a financial institution account with the use of a personal identification number. Modifications or new codes or laws are needed. The Asia Pacific Smart Card Forum is drafting a broad Code of Conduct but its current draft needs much more detailed treatment of these issues, differentiating between accounted and unaccounted SVC systems.

Privacy Issues

The control on collection and use of transaction and other data by smart card operators is of great concern to privacy lobbyists in Australia. Card records could tell where a person was at a particular time, on what transport and what purchases were made. This information may be valuable to law enforcement and

marketers. The Asia Pacific Smart Card Forum's draft Code of Conduct has broad privacy provisions restricting the use of data collected. The Australian Capital Territory legislature this year amended the Territory's Fair Trading Act to prohibit a pre-paid card provider from disclosing to any person particulars of the use of the card where the particulars identify or tend to identify the card user. Privacy rights will need much more negotiation with the federal government recently announcing its intention to extend the federal Privacy Act 1988 further into the private sector.

Law Enforcement Requirements

Law enforcement authorities are concerned about the laundering of money using SVCs which are less bulky and thus less easily detectable than cash. The probable response will be to require a maximum card balance (say $A500) and, perhaps, to require that aggregators of SVC value such as merchants upload the value or most of it to a financial institution account rather than transfer it in peer to peer payments. It is fair to say that law enforcement currently has less concern about fully accountable and identifiable systems such as Visa and Mastercard than it does with Mondex. The Commonwealth Law Enforcement Board has established a Task Force to examine the implications of electronic banking and commerce for law enforcement. The Australian Taxation Office has a similar Task Force.

Remote Banking on the Internet

A number of Australian banks have had home pages on the Internet for some months, advertising their products and services. From 2 April 1996, Advance Bank http://www.advance.com.au has provided transaction services over the Internet to allow customers to transfer funds between their own savings, cheque, credit card and home and personal loan accounts. Customers are issued with a 16 digit Internet account access code and a 4 digit PIN. To access the service, customers must download application software from the Advance Bank site in order to configure the viewer on their Internet browser to show account details and transfer instructions. Advance's target market seems to be high income earners who already have their own PC and private Internet connection.

The funds transfer service builds on existing transaction record and account information services. Once the correct code and PIN have been entered, details of the last 6 transactions on each account are automatically available and, by inquiry, past transactions in the last 7 days, 30 days, or all past transactions on an account can be displayed.

Security is based on (1) a firewall between the bank's host computer and the Internet server and (2) encrypting all messages between the application software running on the customer's PC and the bank computers using public key cryptography (RSA and IDEA 2.2 with 128-bit session keys). Security is the main concern of customers according to Advance Bank and the risks to customers are currently minimised by limiting the access to transfers between the customer's own accounts. However the bank plans to allow payment for external bills next and has licensed smart card technology which could one day permit withdrawal of electronic value onto the smart card via a card reader attached to the customer's PC. Other Australian banks are planning similar services.

Digital Money for Internet Payments

Digital money is a digitised packet of data which serves as either

(1) a **digital coin or note**: the data packet represents the obligation of an issuer to redeem that data packet for a certain amount of "real world" money, against which it was originally issued.

(2) a **digital cheque:** the data packet serves as an instruction by the issuer to a financial institution to transfer the amount of value designated in the data packet from the issuer's account to the account of the "payee" named in the data packet.

Digital money can be transferred over telecommunications lines and computer networks such as the Internet.

Digital money is pure information representing an obligation of a party to convert it into real value. As pure information it needs to be authenticated as having come from the person who purports to have sent it, to be resistant to tampering, counterfeiting and copying and double-spending. Work is progressing on ensuring these attributes through encryption techniques.

Digital money could allow micropayments, for example reading an online magazine or newspaper for 1 cent per page or playing an online computer game for 10 cents per minute, which would revolutionise the type of commerce that could be conducted over the Internet. It would also have the potential to disintermediate traditional financial institutions from the payments system depending upon who was able to issue and redeem digital money on the Internet. It also raises the law enforcement issues discussed above under SVCs.

Presently there are no Australian issuers offering digital money accounts like Mark Twain Bank in the USA. Digicash, the Amsterdam-based developer of ecash, has set up an office in Sydney and is working with financial institutions on such applications, as are other organisations.

One problem with any purely software-based form of electronic money is that the information representing the digital coin or cheque can be easily copied and hence spent multiple times. Recipients of electronic money need to do an on-line check with the issuer that the coin or cheque received has not been previously lodged with the issuer for credit. To do this, the recipient is effectively compelled to deposit the coin or cheque or exchange them for new ones at the issuer, because in a world of potentially infinite copies the first to deposit is the winner. Until the risk of multiple-spending is solved there will not be a freely circulating digital money claim in practice.

Conclusion

The technology behind the new electronic payment systems is still developing. These systems revolutionise and challenge common conceptions of money and cash. Not surprisingly, they raise a host of issues for legal and regulatory systems which were constructed on the paradigms of payments by physical transfers of notes and coin and paper-based account transfers. There is much exciting and challenging work in

reconceptualising existing legal and regulatory regimes to adapt them to the new forms of money and payment.

Cybernews Volume 2, numéro 2 (printemps 1996)

(*) Solicitor and Senior Lecturer in Law, Monash University, Melbourne.
Director, Law of Electronic Banking Project, Monash University.

© copyright 1998 Lex Electronica Tous droits réservés / All Rights Reserved ISSN 1201-7302
