# SUBMISSION TO THE FINANCIAL SYSTEM INQUIRY

# SMART CARDS: CONSUMER ISSUES AND REGULATORY OPTIONS

CONSUMER CREDIT LEGAL CENTRE (NSW) INC.

September 1996

# TABLE OF CONTENTS

**APPENDICES**

## 1. The Consumer Credit Legal Centre (NSW) Inc.

The Consumer Credit Legal Centre (NSW) Inc. is a community legal centre specialising in debt, banking and financial services. The Centre conducts casework and policy research.

The Centre has a strong interest in new technology payment systems, including smart cards, and represents consumer interests in this field. The Centre is an active member of the Smart Card Advisory Network.

This submission was prepared for the Centre by Chris Connolly, with additional material from Anne Stringer.

Anne Stringer
8 September 1996

Consumer Credit Legal Centre (NSW) Inc.
24 Buckingham Street
Surry Hills NSW 2010

tel. (02) 9690 1664
fax. (02) 9319 6050

cclc@mail.mpx.com.au

## 2. Introduction

The Financial Systems Inquiry terms of reference include examination of the likely impact of new technologies on Australia's financial systems. One new technology that is set to have a significant impact in Australia is smart card technology.

Australia is the testing ground for several trials of smart card technology in stored value card systems. Stored value cards raise a number of important regulatory issues, including prudential supervision of card issuers, consumer protection and privacy.

This submission provides an initial overview of these regulatory issues from a consumer perspective. It is hoped that further detail can be added at a later stage in the inquiry.

Many of the issues raised, and the recommendations made, in this submission are also applicable to other forms of new technology payment systems. These include telephone banking, home banking and the transfer of value over the Internet and other on-line services.

In summary, the submission argues that regulatory intervention may be necessary in order to promote consumer confidence in smart card payment systems. Options available to the government include improvements to legislation, promotion of industry codes of conduct and direct supervision of smart card issuers.

The report recommends the establishment of a properly resourced consumer watchdog, either with jurisdiction over all financial services, or particular services including smart cards, and further consultation and research on a number of consumer issues.

This submission also discusses attempts to gain improvements in the terms and conditions of use currently offered to participants in Australian smart card trials.

# 3. Smart Cards

## *3.1 Definition*

Smart cards are plastic cards the size of standard credit cards, which contain an embedded microprocessor chip capable of both storing and processing data. This submission discusses the use of smart cards as "stored value cards", where the chip is used to store and process information which represents value.

Other uses of smart cards include storing and processing medical record information, storing security passwords or biometric identifiers, and storing general identification information.

Smart cards are capable of performing a number of the above functions on one chip. Such cards are known as multi-function cards, and their use is described later in this submission.

## *3.2 Prevalence*

Although invented and patented in 1975, it is only in recent years that smart card technology has become widely prevalent. Expansion in recent years has been very swift. In 1994 there were 420 million smart cards in use around the globe. The majority of these (310) million were as phone cards. Conservative industry estimates predict that by the year 2000 there will be 3800 million smart cards in use, and that around 500 million of these cards will be bank issued stored value cards.[1]

Although no reliable figures are available for the prevalence of smart cards in Australia, the industry estimates that by the year 2000 30% of smart cards in use will be issued in the Asia-Pacific region - about 1200 million cards.[2]

## *3.3 Trials in Australia*

Australia has been chosen by the two largest world card companies as the "guinea pig" for trials of smart card technology. In addition, a number of other smart card trials are occurring in Australia. International media reports reflect the view that Australia is the centre of attention in the smart card field, and that developments here will help shape the world smart card industry.

### *3.3.1 Visa*

---

[1] **Smart Cards: Latest Developments**, Gemplus Technologies Australasia, March 1996.
[2] **Ibid.**

Visa is the world's largest issuer of credit and debit cards. Visa are developing a new product called "Visa Cash" based on smart card technology. They are also considering replacing their existing magnetic stripe credit and debit card systems with smart cards, which they believe will provide enhanced security and functionality.

"Visa Cash" is a complete system of stored value cards - disposable cards, reloadable cards and multi-function cards. Visa began a trial of disposable stored value cards on the Gold Coast in late 1995, and recently extended the trial to include reloadable stored value cards. The reloadable cards can be reloaded at banks, EFTPOS outlets and, in the future, ATMs, from another account, or with cash.

Once again, there are no reliable figures available for the trial. Visa press releases stated that they intended to issue about 100,000 cards during the trial. More recent reports suggest that about 10,000 cards have been issued.

### *3.3.2 Mastercard*

Mastercard have chosen the Canberra suburb of Belconnen for their trial of smart card technology. The trial, which also began in late 1995, involves the issue of cards containing a chip for stored value use, but also carrying a magnetic stripe for debit and credit use.

The three banks involved in the trial (Westpac, ANZ and CBA) each wrote to their existing customers offering them a chance to participate in the trial. Each bank offered separate terms and conditions to customers.

About 2000 people are participating in the trial.

### *3.3.3 Transcard*

Transcard was actually the first stored value card system to begin trials in Australia. Transcard was developed by Card Technologies Australia, and the first cards were issued in the western suburbs of Sydney in early 1995. The cards are reloadable stored value cards which have an emphasis on transport use. Transcard is the only "contactless" system on trial in Australia - the cards are waved over a card reader and read by low frequency radio waves. All other systems communicate through metal contacts on the card and card reader.

About 5000 Transcards have been issued, and the product has been gradually rolled out to a number of suburbs in Sydney's west. The Advance Bank Group (includes BSA) and St. George are both involved in the scheme.

### *3.3.4 Quicklink*

The NSW Government has an agreement with the Quicklink consortium to trial stored value cards in Newcastle. The trial began in late 1995 and about 12,000 cards have been issued. The Quicklink system uses reloadable stored value cards. Several banks and credit unions are involved in the scheme.

The involvement of the NSW Government in a commercial stored value card scheme is highly unusual, and the exact details of the relationship between the Government and the Quicklink consortium are difficult to obtain.

**Further Research Recommended**

What is the nature of the relationship between the NSW Government and the Quicklink smart card consortium?

## ***3.4 Trials Abroad***

There are numerous trials of smart cards abroad. For example, the recent Atlanta Olympics involved an extensive trial of the Visa Cash system. However, there is no other location in which Visa and Mastercard are both introducing smart card systems.

One international product which is very important to Australia is the Mondex smart card system. Mondex is a British system which uses reloadable stored value cards and “Mondex wallets”. These wallets allow individuals to download or upload value from any Mondex card - and value can be transferred from card to card in this way. There is also a Mondex phone which can be used to transfer value between cards.

Mondex is not a fully accounted system - full records are not kept of retail transactions and card to card transfers, although the card itself stores a history of the last ten transactions.

In June this year a number of Australian and New Zealand banks entered into an arrangement with Mondex International to introduce Mondex cards in the Asia-Pacific region.

Another international product which will play an important role in Australia is Digicash. Digicash opened an office in Sydney in early 1996. They promote a product which can be used for secure and anonymous electronic funds transfer on the Internet, and also develop smart card products based on the same concept.

The inventor of Digicash, David Chaum, has discussed the possibility of developing smart cards which create their own digital signatures to authenticate the value being transferred in each transaction.[3] These "digital signature creating" cards would allow an entirely anonymous payment system to operate.

Alternatively, "signature carrying cards" can be used.

Card readers would not need to read a serial number on the card in each transaction. They would instead read the serial number of each "piece" of electronic cash that was being transferred - a serial number (referred to as a certificate) either created by the card itself, or stored on the card.

Digicash are promoting a smart card product known as "Blue". It is a complete smart card software system which uses the chip to store compressed versions of the electronic certificates used to verify Digicash money. A 1K EEPROM card is capable of storing about 500 certificates. Some system specifications appear at Appendix 1.

**Further Research Recommended**

Is a completely anonymous reloadable smart card system technically possible?

[3] David Chaum, Prepaid Smart Card Techniques, Digicash, 1994 and David Chaum & I. Schaumuller-Bichl, Smart Card 2000, Oxford, 1989.

# 4. The Smart Card Industry

## *4.1 The Players*

The big players in the smart card industry to date have been Visa and Mastercard, who have moved quickly to develop smart card systems which can both replace existing products (debit and credit) and offer new functionality (stored value, loyalty etc.).

Visa and Mastercard are both owned by the Banks, however it is often unclear who is responsible for policy direction and product development. Certainly in the smart card field it is the card companies who appear to be making the running, rather than the banks.

Smaller players are the smart card technology companies, like ERG and Security Domain.

Governments are involved both directly (the New South Wales' government contract with Quicklink) and indirectly (the Department of Industry, Science and Tourism's industry support scheme).

## *4.2 Industry Forums*

The major forum in Australia is the Asia Pacific Smart Card Forum which has about fifty members and represents a wide cross section of financial institutions and technology companies. The Forum is currently working on four issues:

- developing an industry code of conduct
- developing standards
- promoting Australian smart card technology abroad
- forming closer links with state and federal governments

A second draft of the proposed Smart Card Industry Code of Conduct will be available shortly.

## *4.3 Directions*

While Australia may be a useful testing ground for smart card technology, the most promising smart card markets are actually abroad. Africa and South America are tipped to leap frog magnetic stripe technology and introduce smart card systems quite quickly. Asia is already proving to be a lucrative

smart card market, with Australian firms winning a number of smart card contracts in the region.

Within Australia there is likely to be a gradual move to replace magnetic stripe systems with smart card systems, and an even slower introduction of new products (stored value and loyalty) based on smart card technology.

The integration of smart cards with other new technology developments such as Digicash and Internet banking may prove to be the real catalyst for industry development. Mondex, for example, have recently developed “add-ons” for computers which will allow customers to integrate Mondex smart card money with Mondex Internet money.

**Further Research Recommended**

What issues will arise from the integration of smart cards with other new payment technologies, including Internet banking?

## 5. Consumer Issues

The Industry and government have recognised that new technology payment systems will only succeed if consumers have the confidence to use the systems. Consumer protection is a vital issue in the development of a successful smart card industry in Australia - and the eyes of the rest of the world are on Australia to see how consumer issues can be addressed.

### *5.1 Benefits for Consumers*

The first question to ask here is, “are there any benefits for consumers?” The smart card promoters have argued that the card will provide the following benefits:

1) Using the card will be quick.

2) The card will be cleaner to handle than cash.

3) Consumers will always have the right change.

There are a number of other claimed benefits for consumers which are dependant on the exact design of the card:

4) Use of the card can be restricted to “approved items”. (For example, a system can be designed to allow a parent to program the card to prevent their child using it at the local video game arcade).

5) The card might store and display a list of the ten most recent transactions.

6) The card might provide enhanced security vis-a-vis magnetic stripe debit cards.

Surprisingly, from a complete review of the promotional literature, these are the only claimed benefits of smart cards to consumers.

## *5.2 Privacy*

### *5.2.1 Anonymity*

In any payment system which is designed to replace cash in low value transactions, anonymity will be an important issue. People believe that as the computer age has advanced, their control over their personal privacy has decreased. The anonymity offered by cash has been one of the last bastions of personal privacy.

Stored value cards are fundamentally different from cash in that not all smart cards guarantee that transactions can be completed anonymously. The level of anonymity depends on the type of stored value card being offered. At the present time there are six types of stored value cards:

1) Anonymous disposable cards with a set amount of electronic value, similar to Telstra phone cards. When the value on the card is spent they will be thrown away (or perhaps collected).

2) Anonymous reloadable cards which can be topped up at banks or EFTPOS outlets (and, in the future, ATMs). These cards do not carry name or address details, and if they are only ever topped up with cash they are likely to remain anonymous. However, customers are likely to prefer to top the card up electronically from their bank or credit card accounts, allowing a link to be made between the card and the identity of the card-holder.

3) Personalised reloadable cards which carry identifying details - perhaps even a photograph or biometric identifier.

4) Multi-function cards which have stored value, debit, credit and/or other functions all on the one card. In the near future they are likely to be hybrid magnetic stripe/smart cards, but in the future all the functions may be on the chip.

5) Mondex type cards which are “semi-anonymous” in that a link can be made between the card and the identity of the card-holder only at each reload stage, and for the most recent ten transactions.

6) Digicash type cards which use digital certificates and can be designed to provide complete anonymity, even if reloadable.

It should be noted that for all these card types it is likely that the customer will sign the back of the card in order to be able to identify the card if it is misplaced or becomes confused with another customer’s card.

A major concern at this early stage of smart card development is that customers may be misled into believing that the cards being promoted as "anonymous reloadable" cards are truly anonymous. This is not the case, and a number of industry analysts have acknowledged that no reloadable card can actually be called anonymous[4]. Nevertheless, the promotional material still refers to such cards as anonymous.

The difficulty with reloadable cards is that if a person chooses to reload their smart card from an EFTPOS terminal, a record will be created showing the details of the reload transaction, including the date, time and location of the reload. A simultaneous record will be created showing the deduction of funds from the customer's bank or credit card account. The two records can be easily linked, and it only takes one such link to compromise the identity of the cardholder for all their previous and future transactions.

**Further Research Recommended**

Does current smart card promotional material tend to mislead consumers about whether or not their card is anonymous?

### *5.2.2 Collection of Information*

Smart card systems will be capable of collecting, storing and processing much greater volumes of personal information than any previous payment systems.

With personalised cards, personal details will be collected at the time individuals apply for their cards. People have become used to providing personal details to banks when applying for credit cards, but are less accepting of supplying personal details to use a product which simply stores their own money. Phone cards and weekly bus tickets are good examples.

Smart cards will generate records of the date, time and location of all transactions. When they were first introduced most smart card promoters focussed on the ability of the cards to create detailed customer profiles for business use as a major selling point to the banks.

Criticism from privacy advocates has resulted in this aspect of smart card technology being removed from most smart card promotional material.[5]

---

[4] Bowcock, Matthew, **Smart Cards and Information Privacy**, Sydney, June 1994.

[5] Compare for example Visa's March 1995 promotional material *"smart cards give the issuing bank a much better understanding of each customer's spending and saving habits and preferences"* and their December 1995 material *"Visa and the issuing banks keep transaction records and personal records entirely separate"*.

However, without any legal regulation of the use of transaction information, the banks and card promoters may choose to create detailed customer profiles at some future stage.

### *5.2.3 Government Agencies*

Smart card operators have responded to concerns about privacy by highlighting the security of the new systems. However, security and privacy are two separate issues which should not be confused. No matter how technically secure the systems are, they will still provide a valuable source of personal information for government agencies - information which was not previously available on this scale or in this detail.

Many government agencies have sweeping statutory powers to access records held by the private sector. These include the Australian Tax Office, the Department of Social Security and the Australian Transaction and Analysis Centre (AUSTRAC).

There has been strong resistance in the past to government plans to use card based systems to identify individuals and to collect information. These same tasks are now being accomplished by the private sector. In Australia only Commonwealth Government departments and agencies are covered by the Privacy Act 1988. The private sector only has to comply with the Privacy Act when it is dealing with Tax File Numbers or conducting credit reference checks. All other activities are unregulated.

### *5.2.4 Other Legal Access*

Obviously, access to smart card transaction records can be granted by the courts to the police, law enforcement agencies and private litigants in civil proceedings.

### *5.2.5 Unauthorised Access*

There is substantial cause for concern in Australia that once a large database of smart card records exists, it may be accessed by unauthorised persons for corrupt purposes. The Independent Commission Against Corruption (NSW) found in its 1991 report that the unauthorised disclosure and sale of information by persons in authority was widespread and systematic. There has been nothing since to discredit that view, and unauthorised disclosures are routinely reported in the annual reports of both the Privacy Committee of NSW and the Federal Privacy Commission.

## *5.3 Consumer Protection*

Smart cards raise general issues of consumer protection - issues which need to be substantially addressed before the systems are implemented and come into widespread use.

### *5.3.1 Consumer Choice*

Choice of payment methods will continue to be an important consumer issue. There is some talk that a combination of new technology payment systems may eventually lead to the "cashless society". Singapore, for example, has indicated that it aims to become a cashless society early next century.

While Australia is unlikely to follow Singapore's lead, there are ways in which consumers may find their choice of payment methods limited.

Pressure to switch to electronic payment systems could come from a reduction in existing services[6] - the closure of bank branches, limits on the use of cash on busses and trains and limits on the number of telephones and vending machines which accept cash.

Also, extra costs may be added to using alternatives to smart cards. Existing systems already discriminate between over the counter and electronic transactions. In addition, merchants and service providers may simply refuse to accept cash or non smart card payments.

These pressures are not fanciful - there are already signs of their presence. Their existence may have an effect on other consumer issues:

> "If consumers are under pressure to make payments electronically, other concerns, for example about privacy, universal access and charges for services, become far more acute, as the choice to opt out of the system becomes less realistic. In general it is in consumers' interests for new services to expand by attracting consumers rather than by pressuring them to change."[7]

**Further Research Recommended**

Does Australian law currently protect consumer choice to use cash in retail transactions?

[6] Federal Bureau of Consumer Affairs, **The Cashless Society?**, Canberra 1995, p. 9.
[7] Federal Bureau of Consumer Affairs, **The Cashless Society?**, Canberra 1995, p. 10.

### *5.3.2 Terms and Conditions*

Unfortunately, due to the absence of other regulatory controls, much emphasis has to be placed on the individual terms and conditions issued by the smart card promoters and the individual banks involved.

The various terms and conditions on offer vary greatly, but are uniformly poor in the area of protecting consumers from liability for card related losses.

In response, the consumer movement has developed a set of ten “Best Practice Guidelines” for the operation of stored value card systems. Their development is discussed below in 8.4, and the actual principles receive close attention at 9.4.

### *5.3.4 Dispute Resolution*

Virtually all current payment systems except cash are covered by available dispute resolution mechanisms. For example, all EFTPOS transactions currently involve a bank or otherwise supervised financial institution, and come within the jurisdiction of the Banking Industry Ombudsman.

Smart card transactions will not necessarily involve a bank or supervised financial institution. Disputes may arise between consumers and smart card promoters or between consumers and merchants and service providers.

An important issue to address will be the various liabilities of participants in each transaction.

Also, the effect of losing a card needs to be assessed. Some smart card promoters are to allow consumers to cancel lost or stolen cards. Others will not. There is obviously a fundamental conflict between privacy and security where lost or stolen smart cards are concerned. One simple principle which could be followed is that those smart cards which offer no anonymity (such as personalised reloadable cards and multi-function cards) should at least offer proper security. It should not be open to the smart card promoters to use “privacy” as an excuse to not provide security on cards which already have no privacy.

### *5.3.5 Costs and Fees*

Banks, card issuers and card promoters have proposed a number of different types of fee structures for smart card systems. It is unclear at this stage who exactly will control fee policy. In the Mastercard trial in Canberra, for

example, all three banks issuing Mastercard smart cards charged different fees

One bank stated in its terms and conditions that it would charge a $1 per month fee after the first two months of the trial. Another bank said they would charge $1.50 per month after the first three months of the trial. The third bank simply stated in its terms and conditions that it would not charge any fee for the first six months of the trial. They did not say what the fee would eventually be. Mastercard did not issue any statement on fees.

Other proposed fees have included:

1) Issue fees

   A one off fee at the time consumers apply for or purchase smart cards, usually to offset the production costs of the cards;

2) Renewal fees

   Annual fees for continuing to use the card which will be automatically deducted from the stored value on the card every twelve months.

3) Transaction fees

   There are several options under this heading. Transaction fees could be calculated as a proportion of the value of the transaction, or there could be a flat fee. They can be payable by the retailer, the customer or both. In either case, the fee will usually be passed on to customers, whether directly or in increased prices.

4) Reload fees

   These reload fees are the fees which are being given the greatest consideration by the smart card operators. A fee is payable each time a customer decides to reload the card. They raise a number of issues. It will be an incentive for customers to put larger value on their card each time they reload to minimise fees. It may also be a “double fee”, as there are numerous fees associated with the EFTPOS, ATM or credit card withdrawal of funds which will be a necessary part of each reload transaction.

5) Monthly fees

   Despite constant criticism of monthly account keeping fees by consumer advocates and the Prices Surveillance Authority, there is discussion amongst smart card promoters of these types of fees. It is likely that the monthly fee would be deducted from the stored value on

the card, or a nominated bank account if the card value was insufficient. Monthly fees have been implemented by the banks involved in the Mastercard trial.

Apart from fees, there will be a number of additional costs borne by consumers as smart card systems are implemented.

No interest will be paid on the funds stored on the smart card. This is despite the fact that the chip is capable of calculating and adding interest without any additional administrative or staffing requirements. The money is in essence a deposit by the consumer of their own funds, locked away until spent. The lost interest over the term of a person's life will be substantial. The benefit which will accrue to the banks from not paying interest on this enormous pool of money will also be substantial. The Reserve Bank of Australia has been critical of the smart card operators' decision not to consider paying interest where it is technically possible to do so. The ACT Minister for Consumer Affairs has accused the banks of "double dipping" because they have signalled that they will charge monthly fees, but will not pay any interest.

The banks will also benefit from reduced cash handling costs and reduced costs from theft.

Any transaction charges for smart cards, however will have a major impact on consumers, especially those already on low incomes and on tight budgets. "If electronic payment becomes the norm, it will be particularly important that charges do not become an unavoidable drain on the resources of low income consumers."[8]

**Further Research Recommended**

**What are the likely fees and costs of for consumers in smart card systems?**

### *5.3.5 Liability*

Many of the liability questions raised by smart cards are similar to the liability questions raised by EFTPOS cards - for example, disputes about "phantom" transactions.

[8] Federal Bureau of Consumer Affairs, **The Cashless Society?**, Canberra 1995, p. 9

However, there may be an additional risk that banks will argue that, because smart cards are so secure, it should be presumed that a card holder must have been negligent if a "phantom" transaction takes place.

The EFT Code of Conduct limits liability to $50 in situation where it is unclear whether the card-holder had been negligent. No such provision currently applies to smart cards.

The terms and conditions of various smart card systems on trial in Australia all offer different levels of protection from liability in different circumstances. This is an area where urgent and extensive work is required.

**Further Research Recommended**

**How can liability issues for consumers in smart card systems best be addressed?**

### *5.3.6 Redemption of Card Value for Cash*

It will be important for smart card users to be able to quickly and simply redeem the value stored on smart cards for cash. Cash may be needed in a number of emergency circumstances (such as paying for food, clothes, medicines, rent, lending family members money etc.) where payment by smart card is unavailable.

A number of smart card promoters have issued terms and conditions in their trials which prevent a card holder redeeming their stored value for cash. This is an unacceptable position. The money belongs to the consumer. The only other time where a person's money is "locked up" in this way is where they decide to place their money in a term deposit bearing substantial interest. As discussed above, smart card promoters will not be paying interest. Even Telstra will redeem the value on a person's telephone card if they believe it is an emergency.

**Further Research Recommended**

Can consumers be assured that their stored value will be redeemed for cash?

# 6. Social Issues

## *6.1 Overextension of Consumer Credit*

Consumer organisations have long held concerns about the consequences of making credit more easily available, and available for smaller and smaller value items, especially where payment is electronic.[9]

Smart cards will allow reloading from credit card accounts or bank accounts in overdraft. So for the first time, credit will be able to be used for small value transactions, such as bus travel , purchasing small grocery items and fast food, and using vending machines, without ever needing to turn the credit into tangible cash.

Payment by electronic means is not tangible. The feelings of loss and gain associated with cash are diminished. Consumers may be encouraged to pay with money they don't actually have and the effect of the loss is not instantly felt. Electronic payments make it difficult to budget - there will be no fortnightly or monthly statements, and individual receipts will be difficult to store and collate.

**Further Research Recommended**

**What measures need to be taken to address the problem of over extension of consumer credit in smart card systems?**

## *6.2 Technology Issues*

Smart cards, despite their general robustness, are still likely to malfunction on occasion. This may lead to a number of difficulties, especially in those systems where no complete record is kept of every transaction, or where the complete record is not "linkable" to a particular card-holder.

Smart card promoters are likely to claim that, like cash, if the card doesn't work then the money is lost, and no-one in particular is liable. This will have obvious disadvantages for consumers.

In the trial of Quicklink smart cards at Newcastle University a student complained that her card was broken, and that she had recently loaded over

[9] National Consumer Affairs Advisory Council, **Overcommitment of Consumer Credit**, Canberra 1982.

$200 on to the card. She asked for the money back. The smart card promoter refused.

The student complained, and was asked to provide a signed statutory declaration that she had loaded the money on to the card and that she had not spent it. The student did not provide the declaration and received no money.

Why she was "scared off" by Quicklink's request is not known. Nevertheless, this example shows the woefully inadequate situation smart card consumers are now in. Quicklink is not a supervised financial institution. There is no appropriate code or dispute resolution procedure in place. Her claim could not be proved or disproved technically because the card itself was damaged. Although a large sum of money was involved, the student was in a situation of complete powerlessness.[10]

### *6.3 Access for People with Special Needs*

People living in remote areas may suffer from a number of the "knock on" effects of smart card systems. The replacement of cash in society generally and the closure of regional bank branches may cause substantial problems if more community consultation does not take place. This submission assumes that such issues are being canvassed in detail in other submissions.

[10] Speech by Peter Flower, General Manager of Quicklink, at the "Computer Money Day" Conference, Newcastle, March 1996.

## 7. ISSUES FOR GOVERNMENT

If smart card systems are allowed to develop in Australia the government will face several important issues of its own.

### *7.1 The Role of Central Banks*

The Reserve Bank of Australia has expressed the view that the main issues raised by smart cards for Central Banks are the integrity of the card issuers, the security and efficiency of the payment system, money laundering, tax evasion, and the possible loss of seigniorage.

For consumers, the most important issue is the integrity of the card issuers. Several of the current smart card promoters are not supervised financial institutions, yet consumers are encouraged to deposit quite large amounts of money on the cards. Both consumers and merchants will suffer if a smart card operator finds itself in financial difficulty.

Improving prudential requirements for smart card issuers should be a high priority for the Reserve Bank of Australia and this inquiry.

This subject is well covered in a paper by Michael Crowley from Monash University published in December 1995 titled “Stored Value: An Analysis of its Institutional and Economic Implications”. This paper appears at Appendix 2.

An interesting proposal for a new role for central banks in relation to “computer cash” is proposed by Graham Wrightson and Andreas Furche in their 1996 paper, “Central Bank Control of Computer Cash”. This paper is unpublished - a draft appears at Appendix 3.

**Further Research Recommended**

**What measures can be taken to improve the integrity of smart card issuers?**

### *7.2 Law Enforcement*

Another important issue for governments is the effect that smart card (and other new technology) payment systems may have on law enforcement activities - especially in the field of money laundering and tax evasion.

Extensive work on these issues is being undertaken by the Electronic Commerce Task Force (chaired by AUSTRAC).

## 8. The Consumer Movement

### *8.1 Academic Research*

A number of Australian academics have been conducting research on smart cards. A list is attached at Appendix 4.

### *8.2 SCAN*

The Smart Card Advisory Network (SCAN) is an informal network of consumer advocates, privacy advocates, government and regulatory representatives, academics and industry members who have an interest in the policy issues which arise from smart cards.

The network meets every two months, and currently has around 100 members. Further details are attached at Appendix 5.

### *8.3 Electronic Money Information Centre*

Developments are currently under way to establish an Electronic Money Information Centre, which would conduct important research on policy issues arising from electronic money, including smart cards. This is a relatively new proposal. More details can be obtained from the author.

### *8.4 Best Practice Guidelines*

A group of privacy and consumer advocates who first met through SCAN developed over a period of time “Best Practice Guidelines for Stored Value Card Systems”. They are intended to promote awareness of consumer issues amongst banks, financial institutions and smart card promoters.

They have been circulated widely for comment, and have received a positive response. A number of organisations have formally endorsed the guidelines:

- Australian Privacy Foundation
- Australian Consumers Association
- Consumer Credit Legal Centre (NSW) Inc.
- ACT Consumer Affairs
- Consumer Credit Legal Service (WA) Inc.
- CARE (ACT) Inc.
- Australian Privacy Charter Council

A copy of the Best Practice Guidelines appears at Appendix 6.

### *8.5 Consumer Representation*

The Australian Consumer movement has tried to involve its members in all aspects of smart card policy development. A list of representative activities appears in Appendix 7

## 9. Regulatory Options

It is now almost a cliché to state that the law in Australia has not kept up with the pace of technological change. This statement is certainly true in the field of smart cards.

### *9.1 Improvements to Legislation*

The federal Attorney General's Department is in the process of establishing an Electronic Commerce Expert Group to examine options for updating legislation which may be relevant to electronic commerce, including smart cards. This will be a lengthy and complicated process.

While little work has yet been undertaken on improving consumer legislation, privacy is an area where improvements have already been proposed on a number of fronts. Unfortunately, none of the improvements are yet in place, and they are unlikely to be implemented before smart card systems develop in Australia.

The federal Attorney General's Department is also currently preparing a discussion paper on extending the jurisdiction of the federal Privacy Act 1988 to include a number of private sector activities.

This change, if implemented, is likely to provide a similar privacy regime to that now established in New Zealand, where the private sector may choose to either accept the privacy principles contained in the Act, or to implement a code which largely complies with the Act and which is approved by the Commissioner. Such codes may be customised to suit particular industries.

These codes take a long time to develop (New Zealand has been preparing industry codes at a rate of about one per year), but once in place they are enforceable.

One difficulty will be whether it is possible to define a "smart card industry" as such that could develop a customised code. Eventually however, all the private sector will come within the jurisdiction of the Act.

The States have long been frustrated by the lack of privacy protection at the state level. New South Wales and Victoria, impatient with the pace of federal developments, have proposed their own legislation. These Acts will cover the state government agencies, and may extend "code based" privacy protection to private sector activities.

### *9.2 Industry Codes of Conduct*

Many of the key participants in smart card systems already subscribe to the EFT Code of Conduct.

The EFT Code of Conduct is a good starting point for developing consumer protection in smart card schemes. It has wide acceptance amongst financial institutions and a structured dispute resolution process.

However, its applicability to smart card transactions is limited.

The EFT Code will only apply if a card transaction is made using a PIN. However, the EFT Code is the subject of a current review. During the course of that review consumer advocates have submitted that the scope of the EFT Code may need to be extended to non PIN card transactions, which will become common after the introduction of smart cards.

Alternatively, consumer advocates have argued for a new code to be established to cover new payment technologies. In an early draft of the Review of the EFT Code the following recommendation appeared:

Draft Recommendation 9.1

> "A federal government working party should be immediately established to consider, in consultation with appropriate consumer and industry representatives, the real and potential impact of new technologies that allow a consumer to transfer funds electronically, but do not require both a card and a PIN to effect the transaction. The working group should assess the potential consumer problems from these new technologies and propose either appropriate changes to the EFT Code to accommodate these technologies or develop a separate mechanism covering new technologies."[11]

This is a recommendation which requires action. This task force should be established urgently, and consumer representatives should be funded to join it.

In the past, consumers, industry and government have been able to work together to establish organisations such as the Banking Industry Ombudsman, and to develop regulatory codes including the EFT Code of Conduct, the Credit Union and Building Society Codes, and a dispute resolution scheme for the insurance industry.

---

[11] Trade Practices Commission, **Review of the EFT Code of Conduct, Interim Report**, Canberra, April 1995.

In developing new co-regulatory, flexible arrangements a consumer voice is essential to ensure they are well designed. Consumer advocates must be funded to ensure their active and meaningful participation.

**Major Recommendation**

**That the new technology payment systems working party, as recommended during the review of the EFT Code of Conduct (Draft Rec. 9.1) be established urgently, and that consumer representatives receive funding to participate in the working party.**

From a privacy perspective, the EFT Code states that card-issuers are to be guided by the principle that customer records are to be treated in the strictest confidence, and that "except where it is provided pursuant to a legal duty or responsibility, no information concerning the use of EFT services by a customer is to be provided by any financial institution, except with the consent of the customer."[12]

This principle is a good starting point for financial institutions. However, as discussed above, the EFT Code will not apply to most smart card transactions, so we must look elsewhere for effective privacy protection.

The Code of Banking Practice also contains confidentiality provisions relating to personal information and transaction information.[13] This will at least provide a level of privacy protection for bank customers where smart cards are issued by banks.

Currently both these codes are voluntary. Their provisions only have the force of law if they are covered in a contract between the institution and the customer (hence the importance of terms and conditions).

The Asia Pacific Smart Card Forum, as a matter of high priority, is developing a Smart Card Code of Conduct. A draft of the Code appears at Appendix 8.

This Code will contain provisions on both general consumer protection and privacy, backed up by sanction provisions and a comprehensive dispute resolution mechanism. Its implementation should add a further layer of protection for consumers - however, the Code will remain voluntary.

[12] **Electronic Funds Transfer Code of Conduct**, 1991, Paragraph 10.
[13] **Banking Code of Practice**, 1993, Paragraph 12.

### *9.3 Company Codes of Conduct*

Although some smart card companies and trial participants have developed (or are developing) codes of conduct relating to privacy, none have shown an interest in codes of conduct relating to more general consumer issues.

Two smart card promoters have issued company specific privacy codes, and three more are working to develop similar codes.

The best of these to date is the Credit Union Services Corporation Australia Limited (CUSCAL) / Quicklink privacy code. It is attached at Appendix 9.

### *9.4 Terms and Conditions*

This is an area where immediate improvements are required. Recognising that the development of codes and other regulatory options may be some way off, representatives of the consumer movement are promoting adoption of the ten “Best Practice Guidelines” for stored value card systems. (See 5.3.2 and 8.4).

The principles are designed to address the most pressing consumer protection issues:

1) Consumers should have a choice as to whether to use a stored value card or other means of payment;

2) Consumer should be enabled to make an informed choice on what type and/or brand of stored value card to use;

3) Consumers should be able to change easily between schemes;

4) Consumer should have current and comparable information on the costs, fees and charges of each stored value card scheme;

These first four principles are designed to enable consumers to choose the smart card type and brand that is most suitable to their needs. They may even choose not to obtain a smart card at all.

5) Consumers should not become liable for large losses in the event of loss or theft of a stored value card;

6) Consumers should not incur any liability due to system failure;

7) Consumers should not incur any liability due to fraud or misuse by an agent or employee of any party involved in system provision or by any other person or body, providing the consumer did not knowingly contribute to the fraud or misuse;

The next three principles aim to protect consumers from becoming liable for losses associated with card use. These principles are a response to some of the early (and some of the continuing) problems associated with EFTPOS transactions.

8) Consumers should have access to an equitable disputes resolution procedure, including access to an external, independent dispute resolution procedure where necessary;

In the absence of other regulatory protection, it is important to provide some means of redress for consumers. With any new technology payment system there are bound to be some problems which the consumers will want resolved quickly, fairly and cheaply.

9) Consumer should have adequate protection regarding the collection, storage, use and disclosure of personal information;

In the absence of other privacy protection, smart card issuers may still offer privacy guidelines or codes which will provide a level of protection in themselves.

10) Consumers should be supplied with terms and conditions which are comprehensive, easy to read and available in appropriate community languages.

Current terms and conditions tend to be either exceedingly brief, or lengthy and dense with legal terminology. The consumer representatives who developed the ten “Best Practice Guidelines” have also begun work on template terms and conditions. These are only at a preliminary stage. They are attached at Appendix 10.

Both the principles and the template terms and conditions are only designed as “stop gap” measures while more effective consumer protection is developed through industry codes and other regulatory intervention.

**Major Recommendation**

**That an existing regulator (ACCC, FBCA or RBA) takes urgent steps to seek improvements to the terms and conditions currently being offered to participants in stored value card trials in Australia. This is an interim measure only.**

### *9.5 Regulatory Structure and Convergence*

There are codes, regulations and areas of contract, fair trading and banking law which cover aspects of the operations of the new technologies in financial services. While some of these have been mentioned above, there are many more.

The convergence of technologies in the financial services field will bring with it jurisdictional problems. In the past, electronic banking systems were proprietary. The institutions owned the terminals and the lines. New developments see the capacity to provide access over non proprietary systems such as telephone lines and through interactive television. The number of points of vulnerability of the network increase greatly, bringing enormous complexity to consumer disputes.

This may mean there is scope for a rationalisation of existing dispute resolution schemes. However, establishing one "super" scheme may be an unnecessary loss of specialised expertise.

Improved inter connectivity between schemes will be required so that consumers are not caught on a back and forth referral loop, or disappear into a jurisdictional black hole. This will require an agreed basis of jurisdiction to ensure consistency and to avoid gaps in coverage. Perhaps there can be a basis on which one regulator can accept the ruling of a different regulator. The Telecommunications Industry Ombudsman might accept a ruling of the Banking Industry Ombudsman in a case where the dispute involves both a financial service and communications technology (and vice versa).

With so many regulatory schemes already in existence, and so many further regulatory options available, it may be worthwhile considering a system which would offer a "one stop shop" to consumers seeking to resolve a dispute.

This does not necessarily have to mean the creation of a super regulator. A secretariat type body, or central bureau could be charged with the initial responsibility of registering consumer complaints. They may undertake referral work or initial investigative work for complaints which involved a wide range of regulatory codes and schemes - privacy, EFT, banking, credit unions, building societies, insurance, credit, smart cards, telecommunications, etc.

The existing and proposed regulatory bodies will still exist, and will be able to develop expertise in their own field. They will ultimately hear and determine the final complaint or appeal. However, the situation will be simplified for

consumers who have a complaint. The central bureau can also perform a number of the less specialised tasks, such as monitoring statistics and education programs.

**Further Research Recommended**

**What options are available to provide consumers who have a complaint about a smart card product with a "one stop shop" for resolving their complaint?**

## 10 A Consumer Watchdog

In this innovative, hi-tech field, characterised by a market which is constantly bombarded with new, complex products, mistakes and wrong turns are inevitable. All consumers of financial services are potentially the losers, paying either from their own pockets or from the public purse for the expensive failures of a profit driven industry.

Some checks and balances are essential. A consumer watchdog, or an independent consumer organisation that will provide an effective third voice in the market place is a simple, cost effective and efficient means of ensuring a fairer market in a way that will not interfere unduly with product development, and that does not require an expensive infrastructure. Such a watchdog will use direct consumer contact and research to monitor the use of new technology payment systems from a consumer perspective, to identify problems and advocate change.

### *10.1 Benefits of a Consumer Watchdog*

A consumer watchdog will ensure the development of better systems, at less cost. Left to develop in an unregulated and unmonitored environment, it is likely that at least some of the systems for supplying new forms of payment will adopt cost effectiveness as a primary consideration and will pay little regard to providing consumer protection, for example the installation of adequate security measures as an integral part of the system.

The potential for large scale loss of public confidence in the payments system if there is one weak link is high. Any inadequacy in a system's security will be quickly flagged if consumer concerns are monitored. If a consumer watchdog is performing a monitoring role, mistakes will be less widespread, and easier and less expensive to remedy at an early point.

With stored value cards, for example, the risk of losses which might occur is currently shifted entirely onto the customer (see terms and conditions). There is little financial incentive for those who design the system to do so in a manner which minimises risk.

It will be recalled that when EFT systems were first introduced customers were liable for transactions beyond the daily limit, resulting in no incentive for banks to ensure that ATMs operated on-line and only allowed withdrawals up to the daily limit. At the time, customers were also liable for all unauthorised transactions, so there was little incentive to improve encryption and pin pad security and design. A consumer watchdog organisation will act as a countervailing voice during system development to ensure that industry is encouraged to adopt long term measures that will minimise future expense to the community and maintain confidence in the payments system.

A consumer watchdog organisation will also encourage better competition. Market forces are unlikely of themselves to produce fair and equitable contractual terms for consumers (for example, it is unlikely that the ability to swap and change between different stored value card schemes will be protected).

A consumer watchdog can monitor industry practices, provide public information, and lobby for greater choice, thus ensuring a more competitive market.

The consumer watchdog organisation will also provide essential and unique information. Government and existing regulators have little direct contact with the experience of consumers in the marketplace. For example, the Australian Payments Systems Council relies on data reports prepared by the banks for its knowledge of market activity.

This data is quantitative and generic - there is no information on the problems experienced by individual consumers, or which financial institution is causing the problem. It is this sort of information which is needed to identify marketplace problems. To collect it an organisation is needed with direct contact with consumers, providing advice, assistance and representation.

### *10.2 Funding*

Government and industry must look for innovative ways to fund the consumer watchdog organisation. One suggestion is that the "slippage" earned on stored value systems should be diverted to fund consumer monitoring and advocacy.

Over time, the slippage is likely to be a substantial sum. There is also the issue of the interest to be earned from the float. The first option should always be to explore ways to repay this income to the card-holders - it is essentially their money - however, if it is not to be repaid, then perhaps it should be diverted to consumer monitoring and advocacy.

In any case, a consumer watchdog organisation will not be a costly investment. The benefits will certainly outweigh the costs. The watchdog might either have a general financial services jurisdiction, or a more limited jurisdiction. At the very least its jurisdiction must cover new technology payment systems.

**Major Recommendation**

**That an independent consumer watchdog organisation be established with jurisdiction to monitor new technology payment systems.**

## 11. Conclusion

The smart card industry continues to develop at a rapid pace. Australia is selling smart card systems to our Asian neighbours with some success, and we continue to host more smart card trials than any other nation.

However, the pace of policy development has been slow. Governments and regulators need to address consumer issues in a timely fashion, in order to protect consumers participating in the smart card trials, and to promote consumer confidence in future smart card products.

The current regulatory options are:

1) Improving legislation

2) Developing Industry Codes of Conduct

3) Improving Terms and Conditions

This submission does not recommend pursuit of any particular option at this stage, although it notes the necessity of improving terms and conditions for consumers already involved in smart card trials as a matter of urgency.

The report sets out areas in which it is believed further research is required, and makes three major recommendations:

**1) That the new technology payment systems working party, as recommended during the review of the EFT Code of Conduct (Draft Rec. 9.1) be established urgently, and that consumer representatives receive funding to participate in the working party**

**2) That an existing regulator (ACCC, FBCA or RBA) takes urgent steps to seek improvements to the terms and conditions currently being offered to participants in stored value card trials in Australia. This is an interim measure only**

**3) That an independent consumer watchdog organisation be established with jurisdiction to monitor new technology payment systems.**

It is to be hoped that consultation between industry, government and consumer organisations will continue, and that consumers will be represented on government and industry forums and committees.

The authors of this report look forward to further opportunities to discuss issues before the Financial Systems Inquiry.

## APPENDICES

## Appendix 1. Digicash Specifications for “Blue”

## Appendix 2. Stored Value: An Analysis of its Institutional and Economic Implications

## Appendix 3. Central Bank Control of Computer Cash

## Appendix 4. Academics Conducting Smart Card Research

Professor Bill Caelli
Information Security Research Centre
Queensland University of Technology

Roger Clarke
Department of Computer Science
Australian National University

Professor Reginald Coutts
Centre for Telecommunications Information Networking
University of Adelaide

Vic Edwards
National Centre for Banking & Capital Markets
University of New South Wales

Jo-Anne Fisher
Centre for Electronic Commerce
Monash University

Robyn Lindley
Department of Information & Communication Technology
University of Wollongong

Dr. Olujoke Longe
Faculty of Law
University of Western Sydney

Mark Sneddon
Faculty of Law
Monash University

Professor Alan Tyree
Faculty of Law
University of Sydney

Professor Anthony Watson
Computer Science
Edith Cowan University (WA)

Graham Wrightson
Department of Computer Science
University of Newcastle

## Appendix 5. Smart Card Advisory Network (SCAN)

The Smart Card Advisory Network (known as SCAN) first met in early 1995. It was founded by the Privacy Committee of NSW who wanted to involve other consumer organisations in policy discussions and research about smart cards.

The Network now has over 100 members, divided into the following categories:

- Academic
- Privacy / Consumer
- Government
- Industry

SCAN meets every two months in Sydney, and invites guest speakers to make presentations on current topics. Speakers have included representatives from every smart card trial (including Mondex and Digicash), the Federal Privacy Commissioner, and a host of other experts.

Minutes and a contact list are circulated, but there are few formalities and no membership fee or structure. SCAN is currently hosted by the Communications Law Centre and coordinated by Chris Connolly. Planning meetings are held every six months.

SCAN has proved a useful forum for an informal, and often frank, exchange of views between the consumer movement, government and industry.

Contact:

Chris Connolly
Coordinator
Smart Card Advisory Network
c/- Communications Law Centre
The White House
University of NSW 2052

tel. (02) 9663 0551
fax. (02) 9662 6839

scan@socialchange.net.au

## Appendix 6. Best Practice Guidelines

### STORED VALUE SMART CARDS

### BEST PRACTICE GUIDELINES

The intention is to provide an environment in which the individual consumer:

1. Has a choice as to whether to use a stored value card or other means of payment;

2. Is enabled to make an informed choice on what type and/or brand of stored value card to use;

3. Can change easily between schemes;

4. Has current and comparable information on the costs, fees and charges of each stored value card scheme;

5. Does not become liable for large losses in the event of loss or theft of a stored value card;

6. Does not incur any liability due to system failure;

7. Does not incur any liability due to fraud or misuse by an agent or employee of any party involved in system provision or by any other person or body, providing the consumer did not knowingly contribute to the fraud or misuse;

8. Has access to an equitable disputes resolution procedure, including access to an external, independent dispute resolution procedure where necessary;

9. has adequate protection regarding the collection, storage, use and disclosure of personal information; and

10. Is supplied with terms and conditions which are comprehensive, easy to read and available in appropriate community languages.

## Appendix 7. Consumer Representation

Consumer representatives currently sit on a number of forums and committees, including (but not limited to) the following:

- Standards Australia Financial Transactions Committee
- Asia Pacific Smart Card Forum Code of Conduct Working Group
- Commission for the Future Smart Card Project Steering Committee
- Electronic Commerce Task Force
- Electronic Money and Gambling Project Steering Committee
- Smart Card Advisory Network
- Electronic Commerce Expert Group
- Service Providers Action Network Electronic Issues Forum

## Appendix 8. Asia Pacific Smart Card Forum Draft Code of Conduct

## Appendix 9. CUSCAL / Quicklink Code of Conduct

## Appendix 10. Template Terms and Conditions

## About the Author

Chris Connolly is a Sydney based lawyer, researcher and consultant, with extensive experience in smart card policy research.

- Author of “Smart Cards: Big Brother’s Little Helpers”
- Speaker at over twenty conferences on electronic money / smart cards / privacy / Internet law, here and abroad
- Author of eight journal articles on electronic money and privacy
- Member of the Electronic Commerce Task Force
- Founder (and current coordinator) of the Smart Card Advisory Network
- Consumer representative on the Asia Pacific Smart Card Forum Code Working Group
- Member of Standards Australia Information Technology Committee
- Member of Standards Australia Financial Transaction Systems Committee
- Member of Gambling and Electronic Money Research Steering Committee

Chris Connolly also gives guest lectures on Internet law at the University of New South Wales (Masters Law Course) and the University of Newcastle (Undergraduate).

He is the Director of the Policy Network, and has recently worked for the Privacy Committee of NSW and the Communications Law Centre (where he still performs part time work).

He was recently invited to represent consumers on the Government’s Electronic Commerce Expert Group.

Chris Connolly
Director
The Policy Network
Level 14, 49 York Street
Sydney NSW 2000

tel. (02) 9262 4237
fax. (02) 9310 0433

chrisc@socialchange.net.au