Consumer Issues in New Electronic Payments

Office of Consumer Affairs
Discussion Paper

October 1996

Consumer Issues in New Electronic Payments

Table of Contents

Executive Summary

Following the successful introduction of on-line debit card systems, financial institutions and others have begun testing the next generation of electronic payment mechanisms which include smart cards, telephone payment systems and Internet payments in the form of on-line banking, secure credit card transactions and "electronic cash". Competition to introduce the new systems is fierce and the pace of development rapid. There will be three smart card pilots under way in Canada in the fall of 1996; major Canadian financial institutions are introducing or expanding on-line banking services; a Dutch company has applied for a licence to launch a virtual banking operation in Canada; and Visa and MasterCard predict their "Secure Electronic Transactions" system, for credit card use on the Internet, will be in operation before the end of the year. This paper provides an overview of the new mechanisms and examines the consumer issues arising from their introduction.

The New Mechanisms

The new systems promise benefits for both business and consumers. Smart cards should reduce fraud losses for issuers, shorten transaction times and reduce the significant costs associated with handling cash. Meanwhile early experiments suggest that an on-line banking operation can cut the overheads associated with conventional banking dramatically. In addition to benefits derived from these efficiency gains, consumers should see improvements in convenience, choice and access to information.

In its most basic form, a stored value smart card is loaded with money by the issuer and used to pay for small value goods and services at retail terminals until its value is used up. More sophisticated cards can be reloaded from the card holder's bank account by the issuer, at automated teller machines, and in some cases via the public telephone system. Meanwhile the National Westminster Bank in Britain and Citicorp in the US have each developed sophisticated, international smart card payment mechanisms capable of large value multi currency transactions. Both are designed to operate over the public telephone system and the Citicorp mechanism is also designed for Internet operations.

Payments over the Internet fall into two general categories: payment for goods and services offered for sale over the net and on-line banking. The former is the electronic technology analogue of mail order. In some cases credit card numbers are supplied, in others "virtual money" systems with names like DigiCash may be used to make payments at the electronic stores. Despite well publicised risks some consumers are providing unprotected credit card numbers for Internet payment. However real expansion of consumer Internet shopping is expected to follow introduction of the Visa and MasterCard SET system projected for the end of 1996.

The first virtual bank, US based Security First, opened its Internet web site (its only branch) last year and claims to offer consumers advantageous interest rates, based on operating costs one third of those for a normal bank. Meanwhile the Dutch based ING corporation has announced its intention to apply for a Canadian trust company licence in order to begin a purely on-line consumer banking operation in this country. A number of existing Canadian financial institutions including Bayshore Trust, Canada Trust, and the Royal and Toronto Dominion banks, the Bank of Montreal and the Vancouver City Savings credit union have also either already begun or are planning on line banking services.

Consumer Issues and Policy Directions

Consumer protection issues for these payment systems fall into the same categories as those which apply to existing mechanisms such as credit and debit cards. They are primarily those of security and privacy, information, liability and redress, and competition and cost.

At the present early stage of smart card development, it seems clear that government consumer protection intervention should be limited. Three major systems will soon be competing for Canadian consumers' business and for the time being the onus will be on suppliers to provide consumer friendly services. However an area for future attention may be the availability of transaction records where bank accounts are accessed by smart cards via public telephones or other terminals not capable of producing hard copy records. In the absence of such records liability and redress arrangements, in instances where card issuer and cardholder records differ, will need careful consideration.

The dangers of transacting business over the Internet are well publicised. Payments system providers are working to eliminate these dangers and will be competing hard to make their systems user friendly. In this area too, while careful monitoring is necessary, the government consumer protection role would for the time being appear limited. However as Internet commerce grows, considerable demand may develop for assurance of merchant reliability and for mechanisms to resolve problems with disputed transactions, particularly at the international level. While in the longer term this may involve development of international standards and agreements, there would appear to be immediate opportunities for consumer and merchant organizations to work together on specific standards for customer service, complaint handling and problem resolution in order to promote a solid Canadian base of consumer-friendly Internet commerce.

The use of public key encryption, as a means of verifying the identity of distant partners to a transaction and the validity of the messages passed between them, is likely to become a mainstay of secure and reliable electronic payment and electronic commerce. The large scale issue of public keys required, implies a need for rigorous management of the processes of issuing keys, maintaining the currency of public key information, and ensuring the privacy and security of private key information. Public confidence in the integrity and reliability of the public key management system will clearly be vital, and government oversight of the development and integrity of the system would therefore appear essential.

There is good evidence that some lower income Canadians experience difficulty in obtaining access to banking services. This evidence bears out concerns expressed by consumer organizations that, in a marketplace where electronic payment becomes predominant, some Canadians may be restricted in their access to everyday goods and services. As there are few signs at the moment of merchants refusing to accept payment in cash for goods and services, this issue is not a pressing one. Nevertheless government should continue to support consumer and other social interest organizations in their present work with financial institutions on access issues.

The impact of electronic technology on the banking and payments field has brought into question existing regulatory requirements for participation in the Canadian payments and clearing system. In particular the potentially instantaneous nature of electronic payments suggests the need for a reconsideration of payment system risks and the rules associated with them. Retailers, insurers and investment dealers are seeking better access to the Interac network, while deposit taking institutions are wary of allowing non deposit taking organizations unrestricted access for reasons related to the security of customer accounts and the integrity of the payments system. Meanwhile, smart cards and secure Internet payments systems could soon provide these groups with more flexible and direct access to their customers than that provided by Interac ATMs. Further research is needed on the consumer implications of broadening the range of institutions which may participate in evolving payments systems, and on the provisions required to ensure the security and stability of these systems.

Finally, government may have a useful role to play in promoting competition through encouraging the development of hardware and software standards which facilitate interoperability of competing electronic payment systems. Such standards should foster competition and innovation by facilitating the entry of new players and increase the efficiency gains from the introduction of the new systems.

In summary, given the rapidly evolving nature of new electronic payment systems, government's present role should focus on:

- careful monitoring of marketplace developments to ensure early identification of consumer problem areas;

- framework policies with respect to payments system access and competition, standards development and public key infrastructure; and

- work with industry and consumer representatives to develop solutions to consumer problems (eg related to information, security, privacy, access and redress) as they are identified. Given the relative speed with which they can be adopted and modified, voluntary rather than regulatory measures may prove more effective in resolving such problems in the foreseeable future.

Introduction

Following the successful introduction of on-line debit card systems, financial institutions and others have begun testing the next generation of electronic payment mechanisms. The new mechanisms include smart cards, smart telephone payment systems, and payments through the Internet involving "electronic cash", secure credit card transactions and on-line banking. These systems hold the promise of significant efficiency gains for businesses as well as benefits for consumers in the form of greater choice, convenience and time savings. If they gain widespread acceptance they will dramatically change the way in which consumers make their everyday payments. The purpose of this study, which focuses primarily on smart cards and payments made through the Internet, is to examine the consumer issues arising from the new electronic payment mechanisms. The paper does not deal with the growth of local computer based barter systems in North America, nor with the money supply and monetary policy implications of these and other forms of electronic payment.

For business, the introduction of stored value smart cards could mean significantly reduced cash handling costs. It has been suggested that cash handling costs for retailers represent 4 to 7% of total costs and much more for service providers like transit authorities which process large volumes of small value payments. The increased speed of transactions will be a second efficiency improvement. MasterCard predicts that a typical smart card transaction could take place in about 300 milliseconds. Losses from fraud may also be reduced through the greater security afforded by chips as opposed to magnetic stripes. Perhaps most dramatic potential savings are those for service providers who can do the bulk of their business on line. For example, the president of US based Security First, the first bank to offer its services exclusively over the Internet, estimates the bank's overhead at 1% of assets versus an industry average of 3 to 3.5%.

Likewise, if consumer acceptance can be predicted from past innovations in payments, the likelihood of success appears high. For example the number of transactions made with a Visa card or MasterCard in Canada has increased in every year since 1977. In the last ten years, transaction numbers have increased by 125% to a total of 840 million transactions in 1995. The use of debit cards at point of sale is a more recent phenomenon but has seen unprecedented success. In the last two years, point of sale transactions have increased by 427%, from 73.9 million in 1993 to 389.2 million in 1995. These numbers show that a great many Canadians are willing to use plastic and on-line transactions if the system proves to be convenient and secure.

Although they have been in use for many years in Europe and Asia, smart cards are just beginning to appear in North America. Smart cards are plastic cards embedded with computer chips. Their electronic memories can hold sizable amounts of information such as bank account balances, credit records, identification and health records; and they can be loaded with a cash value for spending at retail outlets equipped with a suitable terminal. Smart cards have the flexibility for use in a wide variety of applications. For example, the provinces of Ontario and

Alberta are considering them for use as health insurance cards, while British Columbia has begun to use smart cards for security clearance applications in airports for low risk travellers. In the payment area, smart cards offer greater protection against fraud and facilitate electronic payments without the need for on-line authorization via computer at a clearinghouse or the card issuing bank. While smart card technology is likely to be applied eventually to credit and on-line debit cards in Canada, its first major application in this country will be to stored value cards. There are currently four stored value smart card trials taking place or under development here.

The pioneer in Canadian smart card payment applications is Bell Canada. In January 1995, Bell introduced a single use, disposable chip card called Telecarte La Puce in Quebec and Quickchange in Ontario. These, now widely available, telephone payment cards come in various denominations and are designed to be discarded once their stored value is used. A smart card pilot of the British developed Mondex system is scheduled to occur in the fall of 1996 in Guelph, Ontario. Businesses and consumers will be equipped with chip cards used to store money and card reading devices. Consumers will use the card for making transactions the way they would use cash without the requirement of a PIN, signature or online authorization. The Mondex system also enables cardholders to transfer cash over the public telephone system, and Bell is modifying pay phones in Guelph to accept the card. Visa Cash trials began late in 1995 in Toronto and Vancouver and in June 1996 in Quebec and at the 1996 summer Olympics in Atlanta. Visa Cash is a stored value card aimed at small transactions worth ten dollars or less. Targeted merchants include fast-food and coffee outlets, cafeterias, transit, convenience stores, and news stands. Meanwhile the Toronto Dominion Bank and the Bank of Montreal will pilot a stored value card in Kingston, in the fall of 1996, based on the Belgian-developed Proton card system.

Payments over the Internet fall into two general categories: payment for goods and services offered for sale over the net, and on line banking. The former is the electronic technology analogue of mail order. Rather than browsing through a physical catalogue and mailing a cheque or providing a credit card number over the telephone, consumers browse through an interactive on line catalogue or "virtual store" and send electronic payment over the Internet. In some cases credit card numbers are supplied, in others "virtual money" systems with names like DigiCash and CyberCash may be used to make payments at the electronic stores. Despite the well publicised risks, Canadians are currently making credit card payments over the Internet, although the extent of the practice is difficult to determine.

In subsequent sections the paper describes each of the new payment systems which will be available to Canadian consumers, discusses the consumer issues relevant to each and proposes a number of policy directions.

The New Mechanisms

The following paragraphs provide an overview of the new electronic payments systems either currently in place in Canada or likely to affect Canadians in the near future.

Stored Value Smart Card Payments

A smart card typically looks like a credit or debit card but stores information on a computer chip rather than a magnetic stripe. Its relatively larger memory and data processing capacity allows for a broader range of uses for a single card and a greater degree of security in use.

In its basic form a stored value smart payment card is loaded with money by the issuer, and the user subsequently pays for goods or services with the card until there is no money left on it. The cards can be reloadable or designed to be discarded once their initial value is used up. Reloadable cards may be recharged by a bank teller or at an ATM and in some cases are designed to be recharged from the card holder's bank account via the public telephone system. Users may be supplied with a pocket-sized card reading device capable of indicating the balance on the card and providing a record of recent transactions. These basic cards are intended as a means of payment for small value transactions below $10 - a market estimated at $75 billion per year in Canada. However two companies (Mondex and Citicorp) have developed more sophisticated and flexible smart card systems designed to handle larger value payments between individuals and businesses on a global scale.

Bell Quickchange

The smart card's best known Canadian application to date is Bell's Quickchange card, designed to eliminate the need for change in pay phones. This is a single-use card that can be used in any Bell phone equipped with a yellow card reader. Unlike those in many other countries, Bell's phones still accept coins as well as credit and calling cards. Bell has been exploring the possibility of expanding the use of the card to new applications, such as municipal parking meters, but no such arrangements have yet been confirmed.

Visa Cash

Visa also has developed its own smart cards, collectively called Visa Cash. A trial began in Montreal in June this year with about 25 merchants in the Complexes Desjardins, which houses the headquarters of the Desjardins Group, Quebec government offices and several restaurants and boutiques. The pilot involves a disposable card that cannot be reloaded. The first users are Desjardins' employees. Similar trials are operating in Toronto and Vancouver in partnership with Toronto-Dominion Bank and Vancouver City Savings Credit Union. In addition to the disposable card, Visa plans to offer a reloadable version and a more flexible multi function card. The Visa

Cash system will provide a transaction audit trail. Visa is aiming to capture a portion of the Canadian market for small cash transactions of less than $10.

MasterCard Cash

MasterCard international has also developed its own chip card, MasterCard Cash. Trials are currently taking place in Australia. The scheme appears to have been particularly popular with taxi drivers who found it safer than carrying cash. MasterCard has not yet announced a Canadian trial.

Exact

The Toronto Dominion Bank and the Bank of Montreal are planning a Canadian trial of the European Proton card, developed by Banksys in Belgium, this fall. The trial will take place in Kingston. Bell Canada and 800 merchants are participating in the project and the sponsors are aiming to sign up 20,000 customers during the trial. Bell intends to modify 1000 Kingston-area telephone booths to act as smart-card terminals. Consumers will be able to use the card, called "Exact", to pay for calls. They will also be able to use them to download cash from their banks. The banks intend to charge a transaction fee when consumers load their Exact cards, but not when they use them to make a purchase. The loading fee will be roughly equivalent to those charged to users of automated teller machines. There may also be a small fee for holding the card. The Exact card is intended for use primarily in the small-business retail market for purchases under $20. TD Bank and Bank of Montreal have indicated their cards will likely be limited to holding $200 or less.

Mondex

An important and sophisticated smart card system, known as Mondex, was originally developed by the National Westminster Bank in the UK. The system is based on a reloadable smart card but has considerably more flexibility than its competitors and is capable of facilitating worldwide small value electronic payments over the public telephone system. Trials of the Mondex system began in July last year in Swindon in Britain and have so-far involved about 10,000 users. Despite reports of use rates lower than those projected and a delay of the planned introduction of user fees to the initially free service, Mondex anticipates rolling out the service across Britain during 1997. The company has signed franchise agreements for use of the system in India, China, the US, Australia and Canada, and discussions are under way with Japanese interests.

In Canada, the Royal Bank and CIBC have bought the rights to commercialize the Mondex card and will be running a pilot in Guelph beginning in the fall of 1996. More recently Hong Kong Bank of Canada has become a member of the Canadian group. The Mondex card can be reloaded from ATMs and, in the Guelph pilot, via one of the 200 pay phones Bell Canada will soon convert to accept it. The system will enable users to transfer funds between one anothers' cards either by telephone or using a pocket-sized device called an electronic wallet. The card can also be electronically locked to prevent someone other than the cardholder from accessing its stored value. Bell will offer users specially adapted Northern Telecom screen phones for use with the card in their homes. Mondex operators indicate that there is no audit trail of the transactions

made by cardholders, however some consumer advocates suggest that transactions could in fact be traceable. Despite the broad potential and flexibility of the Mondex system, Canadian issuers currently propose that it be used mainly as an electronic purse for small cash purchases, as are most of the other smart cards. After the trial period consumers are expected to pay a small monthly fee in the $1.50 to $3.00 range to use the card, and merchants would be required to rent or purchase a card reader terminal.

Citicorp - Electronic Monetary System (EMS)

Meanwhile Citicorp, one of the largest US banks, has developed its smart card based Electronic Monetary System. EMS lags behind Mondex in terms of its stage of development but Citicorp envisages it will have a broader range of functions. The system is designed to work with computer networks and has the capacity to handle large value transactions in any number of currencies. EMS smart cards can be used to facilitate payments via personal computers and Citicorp has developed one version designed as a secure means of paying for goods and services over the Internet. Citicorp also sees EMS as a viable means of making risk free transfers of large sums between banks.

Internet Payments

The Internet is by nature a wide-open network potentially accessible to anybody who has access to a computer. Access could be made cheaper in the near future with the planned introduction of "dumb" computers designed specifically for Internet use and costing around $500. However, the openness of the network makes possible the interception of communications and the illicit use of the information contained in them. The number of Internet transactions is expected to grow very quickly over the next few years, but reliable growth estimates are not available.

Internet Credit Card Payments

Visa and MasterCard are currently developing a secure system for Internet payment called the Secure Electronic Transaction (SET) system. SET will initially facilitate credit card payment and later be extended to debit card use. The initiative is being undertaken jointly with IBM, Netscape and Microsoft. SET is a protocol that will ensure secure card transactions over open networks. It uses cryptography to provide information confidentiality, ensure payment integrity and authenticate both merchants and cardholders. This protocol is based on RSA data security and uses public/private keys. The American National Standards Institute (ANSI) has created a special group to review and provide comment on the security issues associated with SET. Visa and MasterCard are also co-operating with the International Standards Organization. The aim is to make SET compatible with as broad a range of card systems as possible. Visa. and MasterCard announced a new set of Standards in June 1996 and have suggested that Internet payment systems based on them may now be available to consumers before the end of the year.

Other Internet card transaction systems already exist but are not widely used. The CyberCash

system, for example, works as follows. The technology disguises the credit card number so that it can be decoded only by authorized users such as card issuers. After calling up the Cybercash system on their computers, users type in their credit (or debit) card numbers on their keyboard. The card number is then encrypted at the computer and a code sent to Cybercash that would unscramble the message and present the card number to the issuing bank for authorization via standard electronic channels. Only Cybercash and the issuer have access to the codes to read the numbers. Merchants would receive notification of an approved sale, but would not get the card number. Frequent users may pre-register cards to avoid typing in the card data with every purchase. The Cybercash company imposes a prorated per transaction charge on the merchant.

In Canada, the National Bank and CyberCash have developed an internet payments method called SecurNat. Launched in September 1996, SecurNat allows customers to make purchases from bnak authorized Internet merchants. All information is coded during the purchase transaction, and no credit card information is disclosed to retailers.

Internet Electronic Currency

Electronic currency systems have been developed as an alternative to credit card payments through the Internet. There are a number of variations of which Digicash is a better known example.

Digicash uses tokens that operate something like travellers' checks for the information highway. Users buy the electronic tokens from participating banks, load them onto their own computers and later exchange them for goods and services with participating merchants. The Digicash system has been designed with privacy protection in mind. Transactions are completely untraceable and anonymous, an on-line digital equivalent to cash.

At the beginning of June this year a Canadian company, the Paypro Network, supported by the Canadian Imperial Bank of Commerce announced the development of its own system for secure Internet Transactions. The system will involve the use of debit, credit and smart cards at special terminals attached to home computers.

Finally, in mid June 1996 the Royal Bank announced a partnership with a new Manitoba company and the Manitoba Telephone System to set up the MIX (the ManGlobe International Exchange), a shopping mall on the Internet. Participating merchants will have Web site spots in the mall, which customers can visit using their computers. When orders are placed, ManGlobe handles the transaction, from securing payment to confirming delivery. The Royal Bank is helping to finance the project, has an option to buy part of it and will provide banking services for the operation. The MIX will register customers through a toll-free telephone line and issue them identification numbers. The Royal Bank, VeriFone Inc. and Netscape are working on a new Internet security system which should be ready by the fall.

Home Banking

A number of financial institutions have begun to allow customers to make certain types of transactions (payment of bills, funds transfers between accounts, balance enquiries, and loan and credit card applications) using a home computer. The access can be either through standard phone lines directly to the bank's system, or through the financial institution's World Wide Web site on the Internet.

Virtual Banking

Last year the US-based Security First bank opened its only branch nationwide, an Internet Web site. Its customers can open accounts, make deposits, pay bills, and apply for loans without leaving their homes. For cash withdrawals, clients use ABMs. When a signature is required, the papers are sent by courier to customers. The bank claims it can operate at one third of the costs other institutions must face for maintaining their branch network and can pass savings to customers through higher rates on deposits and lower rates on loans.

Meanwhile the Amsterdam based company ING has announced that it is seeking Ottawa's permission to open Canada's first virtual trust company. ING has experience in virtual banking in the Netherlands and plans to offer services exclusively via telephone and other electronic delivery systems.

Bayshore Trust

Bayshore Trust was one of the first Canadian financial institutions to attempt to use the Internet to reach its customers. It began by offering on-line loan approvals through its Web sites and then began selling GICs. The firm predicts that customers will soon be able to access checking and saving accounts and apply for mortgages. A typical Internet loan application to Bayshore Trust works as follows:

- A customer provides his name, address, employment record and banking information.
- The details are encrypted and transmitted to a central computer , which automatically down loads the applicant's credit record from an on line rating system.
- If the credit record is acceptable, the loan is approved in one or two minutes, subject to reference checks.
- The next day, a courier delivers loan agreement forms for the customer's signature, and funds are subsequently electronically deposited into the borrower's account.

Bayshore believes that the system is fast and convenient for the consumer and keeps overheads to a minimum so that it can charge lower rates than the competitors and still come out ahead.

Canada Trust

Canada Trust was the first of the large established financial institutions to offer services over the Internet. The company has chosen a simple method to ensure a measure of security for customers. The information is displayed anonymously, with no account number, customer name or other identifiers. If messages are intercepted, both the identity of the customer and the accounts remain anonymous. To use the service, Canada Trust customers first registers with the company's telephone banking service. They select their own access code and password which give access to their personal account information.

Unfortunately, a security flaw was found by hackers when CT first began to offer account balance information to customers over the Internet. The flaw enabled third parties to discover individuals' account numbers. CT subsequently developed the present security system based on display of anonymous information.

Vancouver City Savings

VanCity Savings Direct PC and Direct TV will be launched in February 1997 and will allow customers to make bill payments, transfer funds, make RRSP contributions, view account transaction information, and obtain information about VanCity through their PCs or TVs. Equipment for TV will be rented at $6.95 per month. Transaction costs have not yet been determined but are expected to be lower than in-branch transactions

Canadian Banks

Starting in December 1996, the Royal Bank PC Banking and Royal Direct Internet Banking service will allow customers to view account balances, pay bills, transfer money between accounts, and download transaction history. The system may also be adapted to facilitate transfer from an account to a smart card. The Royal plans to charge either monthly or per transaction fees.

The Bank of Montreal's Mbanx is currently available for a range of banking services through the Internet. There is a flat fee of $13 per month for unlimited transactions, although a reward programme based on the value of loans and deposits with Mbanx may offset part of this fee.

The TD, CIBC, and National Bank also presently offer a similar range of banking services. The TD will offer unlimited free banking transactions until the spring of 1997; thereafter, a start up fee and monthly charges of up to $3 for customers with less than $1000 in their accounts may be levied. Transactions such as bill payments will be 45¢ each for those with less than $1000 in their accounts at the CIBC, while the National Bank will charge a $4 monthly user fee.

Consumer Issues

The consumer protection issues arising from new forms of electronic payment fall into the same categories as those which apply to the use of credit and debit cards. They are primarily issues of security and privacy, information, liability and redress, and competition and cost.

Security and Privacy

The fundamental basis of both security and privacy for consumers, in most forms of electronic payment, is information coding or data encryption. Unfortunately the growing power and availability of computers makes cracking codes easier. While encryption can be made more secure by increasing its complexity, this also increases demands on data transmission capacity and senders' and recipients' computer memories. Security experts therefore try to devise levels of encryption appropriate to the worth of the information to be transmitted. The aim is to make breaking the codes troublesome enough by a comfortable margin that the information retrieved would not be worth the effort. Despite occasional and embarrassing flaws in security systems, (like those of Netscape and closer to home, Canada Trust), encryption techniques appear equal to the task of protecting consumer transactions, which tend to be of sufficiently small value to make code-breaking unrewarding. Larger transaction values and therefore large institutions make more rewarding and more likely targets.

However, recognising that encrypted communication between individuals and businesses may become commonplace, security agencies, particularly in the United States, are concerned that their present radio and telephone surveillance techniques could quickly be rendered ineffective. These agencies are pressing for the right and the technological means to decode private messages. There is considerable public debate in the United States as to the appropriate boundaries between citizens' privacy rights in this area and the legitimate law enforcement aims of security agencies.

Smart Card Security and Privacy

Security in smart cards is primarily built into the design of the chip memory, with additional levels possibly programmed in by the card issuer and by the user in the form of a self-selected personal identification number (PIN). While all smart cards may look alike, the sophistication of the security system built into each varies according to the purpose of the card. A simple non-reloadable electronic purse need only establish its own identity and the fact that it contains enough currency to make the required payment. On the other hand a Mondex card, designed to transfer currency to and from bank accounts or other cards, is capable of secure, encrypted chip to chip communication over the public telephone system. The security issues facing consumers in the use of smart cards also vary with the purpose of the card.

Losing a non-reloadable electronic purse is like losing cash. There is unlikely to be an audit trail tracing the record of purchases made with the card, and issuers will not refund any amounts

unused at the time of loss. If the card is reloadable there may or may not be an audit trail tracking its use. Where an audit trail exists the question arises as to whether the issuer should refund any unused balance in the event of loss or theft of the card. Mondex cards are protected by the use of a locking device which prevents further use until the cardholder unlocks it using a PIN. Where cards are protected in this way the unused balance should not be available to a finder or thief and the unused currency will be retained by its issuer. Card issuers in Canada plan to treat the loss of such cards like lost cash and to provide no balance refunds.

The existence of an audit trail for a smart card is regarded by consumer advocates as a mixed blessing. On the one hand the audit trail can facilitate the tracing of disputed payments or potential refund of unused balances on lost cards. On the other hand the absence of an audit trail protects personal privacy, in that the smart card system provides no means of tracking or retaining a record of a consumer's purchases.

A lost or stolen reloadable card which provides direct access to a cardholder's bank accounts presents the same dangers as a lost or stolen debit card. The keys to protection of cardholder accounts are PIN secrecy and early notification of loss so that the issuer can cancel the card. Current PIN security arrangements for debit cards in Canada appear to work reasonably well. Interac survey data suggest that public awareness of the need for PIN confidentiality is high and that the vast majority of cardholders memorise their PINs and keep no written record of them at all. Government and consumer organizations receive very few debit card related complaints annually. However problems may arise both as a result of increasing use of PIN entry at point of sale where the user may be more easily overlooked than at an ATM, and from cardholders' use of easily accessible numbers for PINs, such as birth dates, or telephone or street numbers. The temptation for consumers to use such numbers, or to keep written records of PINs, is likely to grow as the number of security codes used also grows. In the near future it may not be unusual for an average consumer to have to remember separate PINs for an online debit card, a smart card and a credit card, in addition to codes for office voice mail and computer network access and possibly a home security system. PIN security may be approaching the end of its useful life and better techniques may be required in the next few years.

A smart card issue of less direct concern to consumers, is the security of the card against fraudulent loading - the electronic equivalent of currency forgery. However widespread fraud of this kind could clearly cause considerable losses for card issuers and therefore raise costs for consumers.

Security and Internet Payments

Payment by Internet is potentially both very convenient and very insecure. The attraction of near instantaneous access to suppliers world-wide is obvious. However unencrypted messages and unprotected computer files can be accessible to unauthorised users. In addition the potential for fraud is considerable where buyers and sellers are unknown to one another and where payments could be instantaneous or involve the use of credit card numbers. Internet commerce currently presents the same kind of fraud hazards as mail order, but on a larger scale because of the number

of users who can be reached at low cost and because of the speed with which transactions take place.

Major software companies are developing encryption methods which provide sufficient levels of security for large volume use in the open communications environment of the Internet. Meanwhile payments system players are working to minimise the risks that payment could be taken for goods or services which will never be delivered or that credit card numbers can be used fraudulently. AT&T in the US recently announced that it would bear these risks for cardholders who used their AT&T credit card for Internet purchases. More typically, protection efforts involve the payment system operator verifying the credentials of supplier and consumer before they are given access to the system concerned, combined with on line message encryption and payment confirmation. The joint Visa and MasterCard Secure Electronic Transactions (SET) project currently under development is a sophisticated version of this approach. SET payments will be based on encrypted messages. Both merchants and consumers will be assigned certified public and private key pairs, which will verify on-line that users are who they claim to be. Credit card numbers will thus not be transmitted from consumer to merchant.

Secure transactions technology of this kind could transform Internet payment from its currently risky status to a much more flexible and secure alternative to current forms of distance selling. However the assignment of public/private pairs to individuals on a mass basis raises questions regarding their secure and systematic administration. Public confidence in the administration of keys is essential if their use is to become an underpinning of electronic commerce. See Appendix I Canadian Public Key Infrastructure.

Consumer Information

As with other forms of payment, consumers will require sufficient information to maintain financial records, to compare costs and to avoid or resolve problems. The nature of the technology should make the provision of such information both easier and cheaper.

Because they are based on the use of home computers, Internet payment systems should improve the ease with which consumers are able both to maintain transaction records and to compare the costs of competing payment system suppliers. In addition information on consumer and supplier responsibility and liability in the event of problems, and on complaint handling and redress procedures can and should be made easily available on line. Moreover, payment system operators will be in a position to offer consumers information which will make their purchasing decisions easier and more efficient. Citicorp, for example, will incorporate software enabling customers using its EMS smart card for Internet purchases to identify the cheapest supplier of a particular product.

Transaction information required in connection with smart card use will vary with the nature of the card. It seems clear that a non-reloadable electronic purse with a $50 limit is close

enough in nature to cash that no transaction record is required. On the other hand a strong case can be made for the requirement for a printed transaction record when a smart card is reloaded from the cardholders' bank account at an ATM. Cardholders must currently be offered such a record when using an on line debit card at an ATM or at point of sale in Canada.

However the Visa, Mondex and Exact smart card systems envisage accessing cardholders' bank accounts via public telephone, where no printed transaction record will be available. In each system the card will store an electronic record of recent transactions and cardholders will carry card reading devices, but in the event of transaction or card failure, the cardholder will be entirely reliant on the card issuers' record of events.

Information required by consumers on the risks of smart card use, beyond the obvious risk of loss, would appear to be the same guidance which is provided to debit card users on PIN secrecy and prompt reporting in the event of loss or theft.

Liability and Redress

Similarly, cardholder and card issuer liability in the event of smart card problems involving access to a cardholder's bank accounts can be allotted in much the same manner as it is for debit cards in the Debit Card Code. The cardholder would be responsible for maintaining PIN secrecy by not voluntarily disclosing or keeping an undisguised written record of the PIN, and for reporting the card lost or stolen as soon as possible. The card issuer would bear responsibility for ensuring that the card is delivered only to the intended cardholder, for direct losses resulting from equipment problems (including card malfunctions), for any unauthorised access to the cardholders' accounts after the card is reported lost or stolen and for unauthorised access otherwise beyond the cardholder's control.

Since the soon to be introduced generation of smart cards will be used to make most payments at off-line terminals, card issuers will not quickly be able to prevent their use at retail outlets after they are reported lost or stolen. Given the temptation for dishonest cardholders to take advantage of the situation, it would not seem practical for card issuers to accept liability for unused balances on lost or stolen cards of this type. This fact is likely to impose a relatively low ceiling on the amount which consumers will be prepared to carry on a stored value card.

Allocation of liability for problems with Internet payments is likely in the immediate future to be determined by contract between users and payment system operators. Given the pioneering nature of such systems and the well publicised risks for users, this arrangement would seem an optimal one. It seems clear that if the Internet and its successor systems are to realise their potential as media for consumer trade, it will be up to merchants and payments system operators to win consumer confidence. Recent co-operative moves by Visa, MasterCard and software companies to develop SET bear out this contention. So too does the recent offer by the issuers of the AT&T card to bear all liability for loss in the event of transaction problems encountered when

using their card. The card issuer is in this case effectively insuring the card holder against the likelihood of error or dishonesty on the part of the merchant. A safer and more efficient procedure in the long run would likely be positive vetting of merchants by the payment system operator, together with provisions for effective complaint handling and dispute resolution for users of the system. It would seem that there may be parallel potential for merchant associations (such as the Retail Council, the Canadian Federation of Independent Business and the Direct Marketing Association) to establish their own Internet credentials by developing standards for consumer protection and member certification procedures for Internet sales.

Access and Pricing

While Canadian consumers have adopted debit card use enthusiastically, consumer advocates, retailers and others have raised concerns about the pricing of debit card services and access to use of the Interac network, the primary communications channel for debit card transactions in Canada. Representatives of retailers and insurance companies have argued for more open use of the Interac network by organizations other than the deposit taking institutions which currently comprise the membership of the Interac Association. Existing Interac members have expressed concerns that open access to the system by organizations other than regulated deposit taking institutions could pose a threat to the security and integrity of the payments system. One result of these concerns has been the recent Competition Tribunal hearing on access to Interac, which endorsed an earlier Competition Bureau consent order opening up Interac membership and introducing flexibility to rule making procedures and fee structures. However both the Tribunal and the Department of Finance, in its recent consultation paper on the 1997 review of financial institution legislation, have indicated the need for further review of the payments system in light of changes brought about by electronic payment mechanisms. That review will form part of the mandate of a government appointed task force on the future of the financial services sector to be established in the fall of 1996.

Judging by the rapid acceptance of debit cards in Canada (point of sale use exceeds projections by 40% and doubles annually), and by the convenience, security and privacy offered by the Interac system, Canadian consumers have benefitted from the development of a unitary, co-operatively run electronic payments network. Clearly however the cost of these benefits has been the loss of a measure of competition and the degree of access allowed to non deposit taking organizations needs further consideration. Electronic payments have the potential to change the ground rules of the payments system in part because they facilitate instantaneous rather than end of day settlement. Once settlement is instantaneous, it may be that prudential requirements imposed on payments system participants to prevent a domino effect, (resulting from one institution's failure to meet its obligations at the end of the day), can be less stringent. Instantaneous settlement would imply that a failing organization must cease operation the moment it became unable to make a payment, and would therefore be much less likely to undermine the viability of other institutions. In an electronic payments world the participation of non-deposit taking institutions therefore needs careful reassessment. It may be that appropriate prudential and

security requirements for new participants could be established commensurate with the level of risk they pose. It should be noted however, that despite the apparently instantaneous nature of on line debit transactions in Canada (the consumer's account is debited and the merchant's account credited at the moment of sale), the practice of settling for these payments at end of day has been retained.

Smart card technology offers the potential for more immediate price competition because stored value smart card payments need not be cleared, and card issuers need not therefore be participants in the payments system. In some instances organizations other than financial institutions may be better placed to issue smart cards because they routinely process large numbers of small value transactions for an established clientele. Phone companies and urban mass transit operators are obvious examples. The Chicago urban transit authority is introducing a smart card system for use by its customers, which will not result in fare increases or involve additional charges, and which the authority estimates will pay for itself within ten years through savings in cash handling costs. Such organizations not only benefit from reduced cash handling costs but may also be able to offer consumers savings because they have longer use of funds obtained up front in bulk rather than in small amounts when service is delivered. Bell already offers smart cards in Ontario and Quebec. City transit authorities in Ajax and Burlington Ontario now issue smart cards and transit companies in other countries have issued cards which can in some cases be used for a broad range of purchases in addition to bus or train fares.

Just as transit or phone companies can benefit from the use of funds payed in advance for future services, financial institutions issuing smart cards are in a position to benefit from longer use of funds which would otherwise be withdrawn as cash. In some systems the funds are removed from the cardholder's account once loaded on the card, but the card issuing financial institution does not lose access to the funds until the cardholder uses the card to pay a merchant and the funds are subsequently transferred from the card issuer to the merchant's account. The Mondex system involves loading the card with currency issued by Mondex rather than by the card issuing financial institution, and the float is held by the local Mondex franchise. Funds transferred to the card are therefore not identifiable with the bank on which they have been drawn, and can be later deposited by a merchant into his own account without the need for clearing. Bank of Canada figures show that in 1994 approximately $24 billion in paper cash (in addition to bills held by the chartered banks) was in circulation in the Canadian economy at any time, and industry estimates suggest that the annual volume of small value ($10 or less) cash transactions in Canada amounts to about $75 billion. Short term access to even a modest proportion of these funds would appear a worthwhile proposition for prospective card issuers. The benefits of card issuer access to float funds on this scale should clearly be passed in part to consumers and merchants.

The potential benefits of smart card competition to consumers are clear. Governments can foster competition in part by encouraging standardisation so that there is interoperability among systems devised by different issuers, and by ensuring that regulatory conditions imposed on the issue of smart cards by merchants and other non-deposit taking organizations are no more onerous than is necessary to guarantee reasonable levels of system security and consumer

protection. (It should be noted that Interac, Mastercard and Visa are currently working on the development of Canadian smart card standards, with interoperability as one of their objectives.) For consumers, true competition will mean a broad range of issuers offering smart cards that will work at any smart payment card terminal, regardless of the identities of the card issuer and the terminal operator.

Finally consumer advocates have raised concerns that electronic payment methods may not be accessible to lower income and other Canadians, and are concerned that their introduction not result in restrictions on the use of cash. They note that social assistance recipients in particular already have difficulties in cashing government cheques and in opening bank accounts. These concerns, which were noted in the recent white paper on the 1997 financial institutions legislation review, clearly require attention. However a coalition of public interest organizations led by the ACEF du Centre de Montreal has begun working with banks to find solutions to this access problem. Meanwhile advocates for the disabled have also noted that ATM and point of sale terminals are often not accessible to those with disabilities, and that there are opportunities to design in better accessibility as terminals are replaced or upgraded.

Policy Directions and Further Research

The introduction of new electronic payment mechanisms holds the promise of broad benefit to both business and consumers in the form of reduced costs, greater convenience and more secure, reliable means of payment for a potentially vast range of goods and services offered worldwide over the Internet or other electronic networks. Many of the mechanisms are either still under development or in the pilot phase. All are likely to be further refined and more sophisticated products will be developed as users gain operational experience. The following consumer policy directions are proposed recognising both the scope of the benefits to be derived from the new mechanisms and the need for flexibility on the part of policy makers in the current period of rapid change.

Smart Card Consumer Protection Measures

It seems clear that government intervention to protect consumers in their use of smart payment cards should at present be limited. Smart card systems are at an experimental stage and their future development is uncertain. Three major systems are likely to be competing for Canadian consumers' business in the foreseeable future. Under the circumstances the onus will be on suppliers to provide consumer friendly smart card services. However a likely area for future consideration concerns the need for transaction records where bank accounts are accessed by smart cards via public telephones or other terminals not capable of producing hard copy records. In the absence of such records liability and redress arrangements, in instances where card issuer and cardholder records differ, will need careful consideration. It may be that this concern can be dealt with most efficiently by extending the scope of the Canadian Code of Practice for Debit Card Services to cover smart card operations which involve direct access to the cardholder's bank accounts. Smart card transactions of this type would not appear to be very different from those performed using existing magnetic stripe debit cards. Beyond this government should monitor developments closely so as to identify unforseen consumer problems when they arise. In doing so it should seek active co-operation with both industry and consumer representatives in the interests of efficient use of resources and early problem resolution.

Payments System Review

The impact of electronic technology on the banking and payments field has brought into question existing regulatory requirements for participation in the Canadian payments and clearing system. Instantaneous electronic payments and the consequent possibility of instantaneous clearing and settlement, in particular suggest the need for a reconsideration of payment system rules. Retailers, insurers and investment dealers are seeking better access to the Interac network, while deposit taking institutions are wary of allowing non deposit taking organizations unrestricted access to the Interac payments system for prudential reasons. Meanwhile, secure on-

line payments systems, like those under development by Mondex, Citicorp and Visa and Mastercard, could soon provide these groups with more flexible and direct access to their customers than that provided by Interac ATMs. The Government has opened the way for payments system review in its recent white paper on the 1997 review of financial sector legislation. It will be important that careful consideration be given to the value of existing restrictions on the types of institution which may participate in evolving payments systems, and to the provisions required to ensure the security and stability of these systems. Further research is needed on the consumer implications of this issue.

Internet Consumer Protection

The dangers of transacting business and making payments openly over the Internet are well publicised. Internet payments system providers are working hard to eliminate these dangers, are still innovating and will be competing hard to make their systems user friendly. In this area too, while careful monitoring is necessary, the government consumer protection role would for the time being appear limited.

However, as commerce grows on the borderless Internet, considerable demand may develop for assurance of merchant quality and reliability, and for mechanisms to resolve problems with disputed international transactions. There would appear to be opportunities for co-operation between government, merchants, payment system operators and consumer representatives to ensure that such needs are met. In the longer term this may involve development of international standards and agreements. More immediately, given rapid progress toward establishment of secure Internet payment mechanisms, it may be in the interests of both consumer and merchant organizations to work together to develop specific standards for customer service, complaint handling and problem resolution in order to promote a solid Canadian base of consumer friendly Internet commerce.

Access

Present evidence on the difficulty experienced by lower income Canadians in obtaining access to banking services, bears out consumer organization concerns about future access to means of electronic payment. This is far from an immediate concern as there are few signs of merchants refusing to accept payment in cash for goods and services. Nevertheless government should continue to support consumer and other social interest organizations in their work with financial institutions on access issues.

Public Key Management

The use of public key encryption, as a means of verifying the identity of distant partners to a transaction and the validity of the messages passed between them, is likely to become a mainstay of secure and reliable electronic payment and electronic commerce. The large scale issue of public keys required, implies a need for rigorous management of the processes of issuing keys, maintaining the currency of public key information, and ensuring the privacy and security of private key information. Confidence in the management of the public key system would appear as vital to a future society dependent on electronic commerce as confidence in the currency and other aspects of the payments system are today. Government oversight of the development and integrity of the system of public key management would therefore appear essential.

Standardisation and Interoperability

At a time when new electronic payment systems are being introduced with great frequency and are competing for consumer, merchant and financial institution business, it will be in consumers' interests for the competing systems to be interoperative. Interoperability should foster competition and innovation by facilitating the entry of new players and increase the efficiency gains from the introduction of the new systems. For example all smart payment cards should be capable of transacting business with a single terminal at a retail outlet, regardless of the terminal supplier. Currently Visa, MasterCard and the Europay card networks have co-operated to develop common international smart card standards. The Mondex system standards are different and Mondex representatives are optimistic that hardware suppliers will solve the problem by developing terminals which will operate with both types of card, though clearly at some cost. In Canada Interac, Visa and Mastercard have begun joint work on standards for smart credit and debit cards and envisage co-operation with all major stored value card schemes once the work is extended to stored value applications. Government may have a role to play in promoting competition and efficiency through encouraging the development of hardware and software standards which facilitate interoperability of systems.

Appendix

Public Key Infrastructure

Background

As mentioned earlier in this report, security concerns are a major constraint on growth of electronic commerce. Organizations and consumers fear that funds or information will be re-directed or intercepted while in the course of transmission and that they will have no recourse. In order for commerce to function smoothly there is a requirement for security and privacy of information.

Many experts believe that this is only a temporary problem and once encryption and firewalls have been properly designed that the information will be secure.

It is likely that security and privacy issues will be resolved through the use of one or several public key infrastructures (PKIs) currently being constructed by both public and private entities.

Public Key Cryptography

Encryption scrambles data using mathematical formulae so that messages can not be read if they are intercepted. Conventional cryptography consists of a single mathematical key used for encryption (coding) and decryption (decoding) of data, and both the sender and the recipient of a coded message must be in possession the key.

Public key cryptography requires the use of two keys instead of one. One key is kept private and the other key is made public. The information is encrypted by the sender and then decrypted by the receiver using their public and private keys.. The technique can be used both to encode messages so that only the intended recipient can decode them and to authenticate the sender of an uncoded message and verify that the message has not been tampered with en route. The second function is important in commercial transactions where authenticity is essential but where secrecy is not, and where efficiencies can be gained from not encrypting an entire message.

Public Key Infrastructure (Communications Security Establishment Definition)

A Public Key Infrastructure allows secure transmission of financial and sensitive information between relative strangers. A PKI strives to provide authentication, non-repudiation, and integrity, to information technology applications and electronic commerce transactions.

A PKI will be made up of several central systems known as Certification Authorities (CA). These CAs are set up in a tree-like hierarchial structure. Each users' Public Key and identification are placed in a message (certificate). The user's CA will digitally sign each certificate and make the user's Public Key certificate available through publicly accessible bulletin boards (X.500 Directories) along with all other users' certificates. Therefore, any user will be able to get any other user's Public Key from a bulletin board and verify that it is authentic by using the CA's Public Key to verify the CA's signature on the certificate. Certification authorities are in turn overseen by a central authority or root. The root will sign certificates containing the Public Keys of CAs directly subordinate to it and these CAs will sign the certificates of any other CAs below themselves and so on. The process operates quickly on line and establishes a chain of trust among certification authorities and therefore users.

Government of Canada PKI

It is expected the federal government's PKI will be one of the first developed in Canada. The Government of Canada PKI should provide a uniform key management and key certification process for confidentiality and digital signatures across the government. It is planned to be operational in 1997.

The Government PKI project is being developed through a partnership with several departments. These are Citizenship and Immigration, Communications Security Establishment, Department of National Defence, Department of Foreign Affairs and International Trade, Revenue Canada, Royal Canadian Mounted Police, and Treasury Board.