EMERGING FINANCIAL SERVICES TECHNOLOGY: NEW LEGAL ISSUES

Electronic Cash Products: Legal and Regulatory Issues

KARA DALY

Partner
Rudd Watts & Stone, Wellington

INTRODUCTION

It is generally accepted that global electronic commerce using the Internet will be an important area of economic growth in the twenty-first century. To compete effectively in the new global market, banks and financial institutions must plan for, develop and implement new banking and payment systems technologies which are able to predict and meet the needs of both electronic traders and consumers.

The increasing uptake, by banks in particular, of new electronic cash products such as the Mondex and Visa Cash smartcards, and Internet based digital cash systems such as Ecash and CyberCash demonstrates the readiness of financial services providers to participate in the emerging global market. However, one of the principal impediments to the large scale introduction of many of these new technologies is lack of certainty (on the part of both product providers and consumers) as to the legal framework within which these technologies will operate.

In the last few years, there has been considerable discussion and consultation by government and regulatory authorities in this area. Policy and position statements on matters such as cross-border regulation of the Internet, government regulation of cryptography and legally enforceable Internet transactions are now emerging from bodies such as APEC, International Chamber of Commerce, OECD and the United Nations.[1]

However, while the pace with which governments and international bodies are addressing these issues appears to be increasing, many of the legal and regulatory issues facing the banking industry today are not a great deal closer to being resolved than they were a year ago when we

---

1 For example, International Chamber of Commerce Guidelines for General Usage in International Digitally Ensured Commerce (Guidec) (available at http://www.iccwbo.org). OECD's Guidelines for Cryptography Policy (available at http://www.oecd.org); United Nations Commission on International Trade Law (UNCITRAL) Model law on electronic commerce; Report on uniform rules for Digital Signatures, 31st session, New York 18-28 February 1997.

heard a number of speakers at the 1997 Banking Law and Practice Conference address the topic of "Cyberbanking".

This paper updates some of the legal and regulatory issues confronting issuers of smartcard and Internet-based payment systems that were identified by the speakers at last year's conference and examines some of the legal characteristics of those new products primarily from a New Zealand law perspective.

In particular, this paper focuses on:

(1) the central bank's role as issuer of bank notes and coins and how electronic cash products fit within that regime;

(2) the application of the New Zealand Securities Act to electronic cash products;

(3) the security dilemma – the need to prevent and detect fraudulent activity, including the creation and circulation of counterfeit electronic value;

(4) the principal consumer laws electronic cash issuers will need to consider;

(5) the extra-territorial effect of laws in respect of Internet based products in particular, and some of the general policies and position statements of governments and international bodies aimed at addressing this issue.

ARE ELECTRONIC CASH PRODUCTS CURRENCY?

The electronic cash products focused on in this paper are token based payment systems, and in that sense are similar to notes and coins. They are not, however, likely to be treated as currency, for the reasons discussed below.

While different electronic cash products have their own particular characteristics, it can be generally stated that they all rely on advanced technology to store, transmit and receive the digital messages comprising the units of electronic value, they all use sophisticated cryptographic techniques to provide a high level of security and authentication of messages and they all, at some point, require the customer to apply their own funds in exchange for the electronic tokens of value.[2]

To date, the most widely publicised electronic cash product is the stored value smartcard (SVC). A smartcard is a plastic card embedded with a microchip capable of storing and processing vast amounts of information. Smartcards have a wide variety of potential uses but the focus to date has been on developing a software payment application that can sit on a smartcard. Monetary value is loaded onto the card via an ATM, telephone or PC (in the case of Mondex), from the customer's electronic purse. The value on the card can then be used to buy goods and services from merchants participating in the scheme and, in the case of non-centrally accounted SVC's such as Mondex, can be used for person to person transfers of value.

Internet-based electronic cash products, such as Ecash and CyberCash, operate on a PC, lap-top or Apple Mac and involve the secure transmission of digitised data comprising the "coins" or units of value from an Internet bank to the bank account held on the customer's PC. The customer uses those "coins" to buy goods and services from participating Internet merchants who also hold an Ecash account at the online bank.

---

2 See further, the July 1997 draft discussion document published by the New Zealand Inland Revenue Department entitled Electronic Commerce, at http://www.ird.govt.nz, for a general discussion of the characteristics of electronic money.

Whether these products will constitute currency will depend on the relevant laws of each jurisdiction in which the products are used. In New Zealand, the Reserve Bank of New Zealand has sole authority to issue bank notes and coins.[3] Bank notes are defined in the Reserve Bank of New Zealand Act as *"any negotiable instrument used or circulated or intended for use or circulation as currency"*. "Currency" is not defined in the Act but is generally accepted as having certain attributes, not all of which are present in electronic cash products.[4]

"Currency" has been held in Australia to mean "the acceptance, reception, passing or circulation ... of metallic money or government bank notes as a substitution for metallic money".[5] Applying this definition, it is clear that electronic value generated by electronic cash products could never constitute "currency" even though the electronic value will be denominated in monetary units. While electronic cash products are generally designed to be a substitute for cash, the electronic value cannot be compared with metal coins or bank notes and the value may not necessarily "circulate" in the same manner as cash.[6]

It is also unlikely that electronic value would fall within the definition of a "negotiable instrument". While some electronic cash products (such as Mondex) allow free transfer (by delivery) of electronic value, thereby arguably meeting the requirement of negotiability, it is unlikely that electronic value could, without legislation, be considered to be an "instrument". An instrument has historically denoted "a writing" requiring a document of some legal kind. The electronic impulses that make up an electronic payment message would in all probability not fall within that definition.

The result is that, in New Zealand at least, the Crown's monopoly over the issue of bank notes and coins will not extend to the issue of electronic value. Any person is therefore free to issue electronic value in New Zealand.[7]

The position in Australia appears to be similar to that in New Zealand although the wording of section 44 of the Reserve Bank Act 1959 and section 22 of the Currency Act 1965 differs from the corresponding wording of section 25 of the Reserve Bank of New Zealand Act 1989.[8]

---

3 Section 25 Reserve Bank of New Zealand Act 1989.

4 P Ledingham in "Pre-paid cards", *Reserve Bank Bulletin*, December 1994, listed the main attributes of "currency" as: (i) a standard product, easily identified; (ii) risk free (Reserve Bank stands fully behind it); (iii) fully negotiable; (iv) anonymous usage; (v) convenient; and (vi) accepted as valid consideration in all situations. Electronic purses on the other hand are unlikely to be a standard product, will not be risk free and will not amount to valid consideration in all places in all circumstances.

5 Re *Skyring Applications* (1985) 59 ALJR 561, Re *Cusack* (1985) 60 ALJR 302.

6 In practice, when transferring electronic value from one person's SVC or Ecash account to another, the specified amount of value in the transferor's purse is cancelled, and additional units of value are generated in the transferee's purse (although, Mondex value is moved from one purse to another and is not "cancelled"). To this extent, the tokens of value are not "circulating" in the same manner as a bank note or coin.

7 While in New Zealand and Australia there appears to be no legal impediment to non-financial institutions launching electronic cash products, in the UK there is a suggestion that issuers of electronic cash may be required to be a registered deposit taking institution under the Banking Act 1987. If that is so, the application of that law is likely to restrict the electronic cash market in the UK to banks and financial institutions (see further, T C G Tether, "Electronic Cash – The Regulatory Issues", *JIBFL*, May 1997).

8 Section 44 Reserve Bank Act 1959 prohibits the issue by all states and other persons of bills and notes "for the payment of money payable to bearer on demand and intended for circulation"; section 22 Currency Act 1965 prohibits the making or issuing of any piece of metal or other material, of any value (other than a coin issued under authorising legislation) as a token for money or as purporting that the holder is entitled to demand any value marked on it.

ARE ELECTRONIC CASH PRODUCTS DEBT SECURITIES?

If SVC's such as Mondex and Visa Cash, and Internet-based digital payment systems such as Ecash and CyberCash are not, under the present regulatory regime in New Zealand and Australia, currency, how are such products best characterised? It is suggested that the relationship between the electronic cash issuer (or on-seller) and the customer can best be described as a contractual promise by the issuer or on-seller of electronic value in consideration of the payment by the customer of the subscription or purchase price (in real money) to:

(1) credit to the customer an agreed amount of electronic value which the issuer promises will be accepted by approved merchants as a valid method of payment in lieu of real money; and

(2) redeem any unspent electronic value for real money.

On that analysis, products such as Ecash, CyberCash and Mondex SVC's are likely to be debt securities under the New Zealand Securities Act 1978. That Act defines a debt security as any interest in or right to be paid money (or moneys worth) that is, or is to be deposited with, lent to or otherwise owing by any person (whether or not the interest or right is secured by a charge over any property). Therefore, as:

(1) electronic value is subscribed for or purchased by the customer paying real money to the issuer; and

(2) the electronic value represents **money's worth** and, if unspent, is able to be redeemed for real money;

the essential elements of a debt security appear to be met.

That being the case, the issuer of any redeemable electronic cash product must comply with the disclosure requirements of the Securities Act before offering their product to the public in New Zealand. Non-bank issuers will therefore be required to register a prospectus while banks will be able to rely on their General Disclosure Statements published in accordance with the Reserve Bank of New Zealand Act 1989.

The Mondex SVC is slightly different from other electronic cash products in that Mondex value will be originated and issued by a separate entity established in each jurisdiction (the Originator) directly to each Mondex member in that jurisdiction. Members will subscribe for Mondex value by paying cash to the Originator. The Originator will also be required to register a prospectus in accordance with the previously allotted securities provisions in the Securities Act,[9] because the Mondex value will be issued to members with the intention that the value be onsold by members to their customers (who are members of the public).

If an Originator of Mondex electronic value denominated in foreign currency[10] (and domiciled in another jurisdiction) wishes to issue that value in New Zealand, that Originator will also need to comply with the Securities Act or seek an exemption from the prospectus requirements.

It should also be noted that, while the Reserve Bank of New Zealand has indicated that it has no current intention to specifically legislate to regulate new technology such as Mondex, it will continue to monitor developments and, if any significant gaps in the existing disclosure regime emerge, it may recommend additional disclosure requirements for electronic cash issuers over

---

9 Section 6(2) of the Securities Act 1978 provides that all provisions of the Act apply in respect of a security that has been previously allotted with a view to its being offered for sale to the public in New Zealand and the security has not previously been offered for sale to the public in New Zealand.

10 The Mondex SVC is capable of storing electronic value denominated in up to 5 different currencies.

and above the disclosures required by the Securities Act and the Reserve Bank of New Zealand.[11]

In addition to the requirement for a registered prospectus, non-bank issuers of electronic cash products will be required to appoint a trustee[12] (which must be an authorised trustee company or other trustee approved by the Minister of Commerce) who will act for the benefit of the electronic cash customers and monitor compliance by the issuer with any financial and other covenants contained in the trust deed.

The requirement to appoint a trustee will provide, at least in New Zealand, an established regulatory framework to protect the "investing" public from less creditworthy schemes by requiring a minimum level of disclosure in respect of the scheme, the intended use of the "float" (the subscription moneys) by the issuer, the issuer's policies on redemption, security protocols and other information about the general creditworthiness of the issuer.

It will also provide an opportunity for electronic cash issuers to differentiate their products by, for example, including financial covenants in the trust deed, which may include placing limitations on the use of the "float"(and possibly even elevating the ranking of electronic cash holders upon the insolvency of the issuer by providing a first charge over the float). The imposition of such limitations would inevitably enhance the marketability of the product and provide some possible solutions to perceived consumer distrust of these new and largely untested payment mechanisms.

The corresponding position in Australia under the Corporations Law is somewhat less clear. While the definition of "debenture" in section 9 of the Corporations Law[13] is similar to the definition of a "debt security" in the New Zealand Securities Act, it has been suggested in Australia that electronic cash products may be able to be structured to avoid coming within the definition of "debentures" for the purposes of the Corporations Law,[14] presumably by treating the transaction between the electronic cash issuer and the customer as a purchase of goods or services rather than as a deposit of money which is able to be redeemed by the customer upon demand.

TAX ISSUES

It has been suggested that, because of the global nature of the Internet and the trend towards globalization of commerce on the Internet, traditional concepts of residence for tax purposes and source of income will be difficult to apply to Internet-based cross-border transactions, in particular because of the potential difficulty in determining the true source of a communication. In addition, particularly with anonymous transactions, there is a potential tax evasion or avoidance risk that must be addressed by tax authorities.[15]

The New Zealand Inland Revenue Department (IRD) has produced a position paper on taxation and the Internet,[16] which addresses some of these issues. The IRD has stated that it will apply the principle of neutrality in connection with the supply of goods or services over the Internet, so that

---

11 Supra, note 4.

12 Section 33(2) Securities Act 1978.

13 "Debenture" is defined in section 9 of the Corporations Law as a document issued by a body corporate evidencing or acknowledging indebtedness of the body in respect of money deposited with or lent to the body whether constituting a charge on the property of the body or not (other than, amongst other things, a cheque or order for the payment of money, bill of exchange, promissory note exceeding $50,000 or bank deposits).

14 A Beatty and G Hammond, "Smartcards: An Australian Perspective", *JIBFL*, July-August 1997.

15 A useful discussion of these issues is set out in the IRD's paper on Electronic Commerce, supra note 2.

16 New Zealand Inland Revenue Guidelines to Taxation and the Internet 1997, http://www.ird.govt.nz.

a service provider who does not have a place of business in New Zealand and who provides services via the Internet from an offshore website will not be required to deduct Non-Resident Contractors Withholding Tax from the price payable for those services, on the basis that the services are performed offshore. In addition, an offshore website will not fall within the definition of a fixed or permanent place of business in New Zealand for the purposes of the Goods and Services Tax Act 1985, so long as the website service provider is a non-resident.

The paper concludes that, for tax purposes, there is no difference between a transaction performed electronically and a traditional manual transaction. It is the commercial reality which will determine how the electronic service provider of the future will conduct its affairs, not solely as a result of taxation minimisation plans.

The IRD has, however, acknowledged that the issue of taxation of on-line transactions is unlikely to be easily resolved on an international basis when different countries may treat an Internet transaction such as the purchase and downloading of software variously as a sale of goods, a provision of services or a licence of intellectual property rights, each with differing tax consequences. In addition, the use of mirror sites or servers in more than one country will make appropriate tax treatment difficult as customers will not necessarily know the actual location of the server with which they are interacting.

Quite apart from the difficult conceptual issues faced by the IRD in connection with taxation of business transactions conducted on the Internet, it is apparent that governments and international bodies are keen to encourage the development of global electronic commerce. To this end the US Government, and more latterly, APEC, have voiced support for the development of the Internet as a tariff-free zone and have agreed in principle that no special taxes should be applied to Internet related transactions. Whether this stance proves to be successful remains to be seen, as it appears that the European Union is considering introducing "bit tax" on transmissions of digital information.[17]

RISK OF FRAUD AND COUNTERFEIT ELECTRONIC VALUE

One of the biggest threats to the success of electronic cash products is the risk of counterfeit electronic value circulating without detection by the electronic cash issuer, with the result that the integrity of the electronic cash is jeopardised, potentially leading to loss (by either or both the customer and the issuer). Ultimately, if the electronic cash issuer is required to redeem both counterfeit and original electronic value, the assets of the issuer may not be sufficient to meet all claims, resulting in the insolvency of the issuer.

Both product developers and government authorities are concerned about this risk, given the ease (in the absence of sophisticated security systems) with which the digital information comprising "electronic value" can be copied. Developers of electronic cash products have adopted a variety of techniques to prevent and/or detect counterfeit electronic value. These techniques generally involve the use of public key/private key cryptography to ensure private authenticated payment messages between sender and recipient (thereby preventing a third party from recreating that message) and/or to give each payment message a unique number or characteristic so that, if it is fraudulently recreated, the recreated payment message is immediately identified as counterfeit. Some of the solutions adopted by various product developers are summarised below.

CyberCash is a fully audited Internet based payment system in which the customer, the Internet merchant and the CyberCash payment server all use digital signatures[18] to authenticate

---

17 Jonathan Schawz, "The Tax Haven in Cyberspace – Export Law", *Financial Times*, 17 April 1997.

18 A "digital signature" is created when a message is sent from one person to another, including a "message digest" generated by performing a computation using the sender's private key and the message. The recipient performs the inverse computation using the public key. If the two match, the signature is valid.

transactions. The CyberCash customer creates and uses a unique identification which is registered with the CyberCash payment server using public/private key encryption. The customer can use CyberCash to purchase goods and services over the Internet only where the customer's payment request has been signed by the customer's private key. This system does not provide customer anonymity but does provide an audit trail which will enable tracking of fraudulent transactions.

Ecash (by Digicash Inc) by contrast, is an Internet based payment system which offers customer anonymity but can trace fraudulent use of Ecash coins by the use of "blind signature" technology.[19] Ecash customers withdraw digital coins from their Ecash account and store them in their Ecash wallet software (on their PC). The wallet software keeps a record of all the customer's transactions and gives each digital coin deposited in the account a unique serial number. The Ecash bank then validates the coins with the bank's blind signature. As the bank cannot connect the serial number of a coin it signs with the customer to whom it is being issued, the customer's identity remains unknown to the bank. The Ecash bank will keep a "spent-coin" database and a list of all coin numbers that have been spent to prevent multiple spending of coins.

The problem with this system is that while it identifies counterfeit value, the bank cannot identify the fraudulent customer. The proposed solution to this problem (while retaining customer anonymity) will require a customer to answer a random numerical query on each digital coin when spending it. Legitimate transactions involving digital coins will remain anonymous, but as soon as a coin is spent twice, the bank should be able to identify the spender, using the information gathered from the random numerical query.

Smartcard technology has also developed to provide both accounted (non-private) and unaccounted (private) systems which have different design features to prevent and detect fraud. Visa Cash is a fully accounted system requiring transactions to be sent to the issuing bank for verification and authorisation, with the result that fraudulent transactions should be identified and stopped prior to completion.

Non-accounted SVC's such as Mondex do not require bank authorisation. However, while commentators have differing views, it is generally acknowledged that the security protocols adopted by Mondex are extremely sophisticated.[20] Each Mondex card will contain two different security protocols, the intention being that the card issuer may rotate the security protocols from time to time by deleting the active system, activating the dormant system and then transmitting a new dormant system to the card. The rotation of these security protocols could potentially isolate and shut down fraudulent use of cards.[21]

In New Zealand, as electronic cash products will not constitute bank notes and coins, the anti-counterfeiting provisions in the Reserve Bank of New Zealand Act 1989 and the Crimes Act 1961 will not apply to electronic cash products. Accordingly, if the technical features of any electronic cash product designed to prevent counterfeit of electronic value are not successful, then

---

19 Blind signature technology is a method that allows a person or an organisation, such as a bank, to apply its digital signature to a message without seeking its contents.

20 David C Stewart, in a paper entitled "The Future of Digital Cash on the Internet" (*JIBC*) states that: "Once in use, no other chip card or hardware device posing as a Mondex card could interface with a real Mondex card. Mondex cards detect spoofs and refuse to transfer money to them. The system relies on the fact that each card is certified by a Mondex digital signature. The transfer process itself is also extremely secure. When a transfer occurs, the two cards not only verify each other's authenticity, but the transfer occurs in a sequential process so that funds cannot possibly exist in two places at once."

21 See further Robert D Fram, Margaret Jane Redin and Thomas P Brown, "Altered States; Electronic Commerce and Owning the Means of Value Exchange", (available at www.hewm.com), for a detailed description and analysis of the various electronic payment mechanisms and the encryption techniques and security protocols adopted by each of them.

prosecution under the general crimes of fraud and forgery in the Crimes Act would be the only alternative.[22]

The use of Internet-based payment technologies for money laundering transactions is also a major concern for law enforcement agencies.[23] In New Zealand the Financial Transactions Reporting Act 1996 places obligations on financial institutions to report to the police suspicious transactions which may involve money laundering. While the Act is principally concerned with cash transactions (requiring automatic reporting of all transactions involving cash in excess of $10,000) it also applies to any transaction (whether or not involving cash) where the financial institution has reason to suspect that the transaction may be relevant to the investigation or prosecution of any money laundering offence.[24]

The Act places a statutory obligation on financial institutions to verify the identity of customers at the time an account is opened (usually by means of documentary evidence).[25]

"Cyberbanks" which offer an online account opening service need to consider carefully how they can comply with these statutory requirements, particularly in respect of products that are designed to preserve customer anonymity.

CONSUMER LAW

Issuers of electronic cash products must also consider the relevant consumer laws that will apply to the issue and use of electronic cash. In New Zealand, these laws are, to a large extent, contained in the Consumer Guarantees Act 1993, the Privacy Act 1993 and the Fair Trading Act 1986. The New Zealand Code of Banking Practice will also apply in respect of bank issuers.

Privacy Act 1993

One of the biggest consumer issues that electronic cash issuers will face is consumer resistance and distrust of SVC and Internet-based payment systems because of their potential threat to personal privacy and autonomy. This distrust largely arises out of the inherent openness of the Internet as a communication medium and the potential for issuers (and others) to use smartcard and Internet-based technology to collect and collate vast amounts of personal information and use that information for a variety of purposes both authorised and unauthorised.[26]

In New Zealand, consumers should take some comfort from the protection afforded by the Privacy Act 1993, which requires collectors and holders of personal information to make it known to the

---

22 The crimes of false pretence, obtaining credit fraudulently and dealing with documents with intent to defraud are likely to be the principle crimes in respect of counterfeit electronic value without further specific legislation.

23 Stephen R Kroll, Legal Counsel, Financial Crimes Enforcement Network US Depart of the Treasury, "Some thoughts on Law Enforcement and Stored Value Products" (1997) 1 *JIBFL* 3: "These systems combine the speed of the present bank-based funds transfer system with the anonymity of currency ... Smartcard transactions and international payments transacted over the vast Internet system could be immediate, effected in multiple currencies, conducted entirely outside of the traditional funds transfer channels, and encrypted with a strength that makes them completely unreadable for all practical purposes."

24 Financial Transactions Reporting Act 1996 section 15. (However, the Act's crossborder provisions will only apply to real cash transactions, so e-cash transactions will not be caught.)

25 Ibid, sections 6 and 12.

26 It should be noted, however, that electronic cash products may have characteristics which preserve personal privacy and which do not allow those who come into contact with the customer (eg: merchants, issuers, etc) to gather any meaningful information about the personal identity or spending habits of the customer.

individual the information that is being collected from them, the purpose of the collection, who will hold the information and their rights of access and correction. Issuers of electronic cash and SVC's will be required to obtain the consent of customers to the particular uses for which that information will be used and to the disclosure of that information to third parties. Consumers, theoretically at least, should then have the necessary information with which to compare the various privacy protection mechanisms offered by electronic cash issues and select between them.

The New Zealand Privacy Commissioner has acknowledged that the biggest privacy risk relating to advanced communications technology is the control over information in large centralised databases which can store information gathered from hundreds of transactions and allow those who have access to the information to build profiles of individuals and their personal spending habits. However, provided security measures are strict and Ecash issuers are responsible about the use of information collected from consumer transaction, the privacy risk, at least in countries adopting broad based privacy laws, should be a manageable one.

Consumer Guarantees Act 1993

The Consumer Guarantees Act imposes a number of statutory guarantees on providers of goods and services which are ordinarily acquired for personal, household or domestic use. The guarantees include a guarantee as to the fitness of a product or service for a purpose made known to the service provider, a guarantee that a reasonable level of skill be used in providing the service and the guarantee that the service will be provided in a timely manner and at a reasonable cost.

As electronic cash products rely on sophisticated computer and software systems, third party networks and other third party providers, electronic cash issuers should be aware that, in the event of computer malfunction or network failure, they may have an exposure under the Consumer Guarantees Act for breach of the guarantee that the service will be provided in a timely manner and at a reasonable cost. The "reasonable level of skill" guarantee used may also be breached in these circumstances. These guarantees are not able to be contracted out for non-business customers and will apply notwithstanding any specific terms and conditions applying to the use of those technologies.

Fair Trading Act 1986

Section 9 of the Fair Trading Act, (the equivalent of section 52 Australian Trade Practices Act) prohibits misleading or deceptive conduct in trade. Issuers of electronic cash products will need to be careful to ensure that no misleading impression is given in promotional material that their product is "cash" or even that it is equivalent to cash. The ultimate value of an electronic cash product will depend upon the creditworthiness of the issuer. Comparisons with "cash" could therefore be misleading in that cash (ie bank notes and coins) is legal tender and effectively has the guarantee of the sovereign state that issued it. This "guarantee" will not apply to electronic cash products.[27]

Furthermore, care will need to be taken in describing the operation of the relevant system, the security protocols applying and the risk of loss to the consumer. Overselling the degree of security offered by the product may amount to more than mere "puffery".

---

27 This point is made by P Ledingham, Reserve Bank of New Zealand, in his article on prepaid cards, supra, note 14.

Code of Banking Practice

Smartcards are specifically included in the definition of "Cards" in the New Zealand Code of Banking Practice. The Code states that the usual limitation on a customer's liability in cases of theft ($50 where the customer has not acted fraudulently or negligently or contributed to any loss of a card) may **not** apply to stored valued cards or the stored value function of a multifunction card. It is therefore anticipated that for stored value cards like Mondex, loss as a result of a stolen or misplaced SVC or the unauthorised use of a SVC is likely to be borne by the customer and not the bank (consistent with its "cash" like characteristics).

However, the Banking Code of Practice also specifies that the customer will **not** be liable for loss caused by:

(1) fraudulent or negligent conduct by employees or agents of a bank or parties involved in the provision of electronic banking services (which will include third party network providers);

(2) faults that occur in the machines, cards or systems used, unless defaults are obvious or advised by the message or notice on display;

(3) unauthorised transactions occurring before the customer has received their card, pin or any password; and

(4) any other unauthorised transaction where it is clear that the customer could not have contributed to the loss.

The Code therefore extends to SVC's the notion that banks assume the risk of loss through system malfunction or the fraudulent conduct of a third person.

In respect of Internet based digital cash products, the Code of Banking Practice provides generally that where "other payment services" are provided, the bank will inform the customer of any conditions of use that apply to the payment service offered, including the issue and security of cards, card numbers, pins or passwords and the liability resulting from a breach of those conditions, any applicable fees, the deadline by which the customer may alter or countermand payment. These provisions do not specifically deal with the issues that are likely to arise if a bank introduces an Internet-based payment system such as Ecash. The Code of Banking Practice is, however, updated on a regular basis and is likely to be amended to take account of these new technologies.

JURISDICTION

The above discussion of the application of New Zealand laws to electronic cash products illustrates the extent to which the laws of one jurisdiction can dictate the structure of electronic cash products for that market. If the product is an Internet- based one, care must be taken to limit the geographical market for the product to those jurisdictions whose laws the issuer is satisfied it can comply with.[28]

The dangers of soliciting business on the Internet without adequately considering the potential audience and including appropriate limitations of liability and choice of law clauses is aptly

---

[28] By way of example of the pitfalls of not complying with local laws, the US Securities and Exchange Commission has recently ordered that a number of public offerings of securities over the Internet (from locations outside the USA but with no restriction on an applicant's residence or jurisdiction) be immediately withdrawn because they had not registered with the Securities and Exchange Commission as they were required to under the Securities Exchange Act 1934 (see www.freemarket.org and www.ocr.ltd.bs).

demonstrated by a number of recent US cases which have imposed (civil) jurisdiction in respect of on-line offers of products and services from web sites located out of state.[29]

These cases, while turning on their facts, have found fairly consistently, that where the level of interaction with a person in another state is sufficiently high, the responding state will have jurisdiction and the (civil) laws of that responding state may also apply to the web site owner. Factors that may be considered in determining jurisdiction will include:

(1) the quantity of contacts within the forum;

(2) the nature and quality of those contacts;

(3) the connection and the cause of action with the contacts;

(4) the interest of the state in providing a forum; and

(5) the convenience of the parties.[30]

These US cases demonstrate the risks associated with determining jurisdiction in respect of disputes involving Internet trading, which, together with the potential for jurisdictions to pass inappropriate laws relating to Internet activity, raise difficult conflict of laws issues which may hamper the natural growth of the global business community.

There are now a number of international committees and organisations looking at these issues to determine the most appropriate way to encourage the development of global electronic commerce and to address some of the difficult legal and regulatory issues from an international perspective. The prevailing view is that the private sector must continue to lead in the development of electronic commerce and a non-regulatory and market oriented approach should be taken to avoid unnecessarily limiting the availability of products and services to consumers around the world, and distorting the development of the electronic market place.[31]

However, electronic banking and payment systems are considered to require a more interventionist approach to ensure that issues such as payment security and law enforcement are adequately dealt with. The US government policy position in respect of electronic payment systems was summarised in a 1 July 1997 Whitehouse paper on global electronic commerce as follows:

> "At this early stage in the development of electronic payment systems, the commercial and technological environment is changing rapidly. It would be hard to develop policy that is both timely and appropriate. For these reasons, inflexible and highly prescriptive regulations are inappropriate and potentially harmful. Rather, in the near term, case by case monitoring of electronic payment experiments is preferred. From a longer term perspective, however, the market place and industry self regulation alone may not fully address all issues for example, Governmental action may be necessary to ensure the safety and soundness of electronic payment systems to protect consumers or to respond to important law enforcement objectives."[32]

---

29 For example, see *Inset Systems Inc v Instructions Set Inc* (937 F Supp 161 (D) Conn 1996); also *Maritz Inc v Cybergold Inc* (BNA Electronic Information Policy and Law Report, Ramsey County District Court File No C-6-95-7227, December 11, 1996, Vol 1 at 587; No 4:96CV01340 (Ed Mo Org 19, 1996) *State of Minnesota v Granite Gate Resorts*.

30 Ibid – State of Minnesota v Granite Gate Resorts.

31 This view was promulgated by the Federal US Interagency Taskforce in its draft report on developing guidelines for electronic commerce.

32 A Framework for Global Electronic Commerce, The Whitehouse, July 1 1997.

More recently, at the APEC leaders meeting in Vancouver in November 1997 the United States proposed that by January 2000, APEC should have in place:

(1) a consistent approach to tariffs and taxes for electronic commerce;

(2) a uniform commercial code for electronic commerce;

(3) intellectual property protection for the Internet;

(4) technologies which empower consumers to limit content they do not wish to receive;

(5) a market driven means for developing technical standards;

(6) a common, market driven approach to electronic payment systems;

(7) a duty free Internet;

(8) means to ensure the security of digital communications, networks and transactions.

With these and other international initiatives,[33] the financial services market and business generally can assume that heavy handed regulation of the Internet is unlikely to occur and the present uncertainty and disparity between local laws applying to Internet transactions, including Internet payment mechanisms, may yet be addressed by way of international treaties and conventions.

CONCLUSION

This paper has addressed some of the fundamental legal and regulatory issues facing developers of electronic cash products and has expressed some views with regard to the ways in which such products will be treated under New Zealand law. However, in order for global electronic commerce, including these new global payment mechanisms, to become the accepted norm for conducting business, many of these issues will need to be dealt with on an international level, given the potential for the issues identified, both in civil and criminal contexts, to give rise to complex and novel questions of jurisdiction and conflict of laws.

The recent signs are that international consensus on these issues is viewed as highly desirable, if not imperative. There is hope therefore that as SVC's and other electronic cash products gain a wider public acceptance and market penetration, the present uncertainties and unresolved legal and regulatory issues should be addressed within a more reliable legal and regulatory framework, incorporating a combination of industry self-regulation, international conventions and (light-handed) domestic legislation.

---

[33] Supra, note 1.