CYBERBANKING: THE EMERGING TECHNOLOGY AND LEGAL ISSUES

Cyberbanking and Payment Products: Legal and Regulatory Issues

MARK SNEDDON

Associate Professor of Law
University of Melbourne Law School

INTRODUCTION

The Internet presents many opportunities and some challenges to financial institutions. Currently, financial institutions are utilising the Internet for three broad types of application.

First, the Internet can be used as a vehicle for advertising products and services and for requesting information (including loan applications) and many Australian financial institutions have home pages on the world wide web for these purposes.

Secondly, it can be used as another means of providing remote account access services for account inquiries, funds transfer, lending and bill payments to third parties, in the same way the telephone system is currently used for telephone banking services and personal computer banking using telephone links.

Thirdly, the Internet can be used as a means of transmitting digital payment instructions or representations of value direct from payer to payee, rather than to a financial institution. (Clearing and settlement of these payments may need to occur through financial institutions.) These direct payments may use:

1. existing off-Net payment mechanisms eg payer transmits credit card details or a key that links to the credit card details.

2. new on-Net payment mechanisms which may be:

    (1) encrypted software-based, ie a packet of digitised data, eg

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

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

(2) a hardware/software combination – eg smart card in a card reader attached to a personal computer can be used to transmit electronic value from card via Internet to a payee or receive payments.

This paper focuses on the second and third applications mentioned, namely using the Internet as another means of remote access to financial institution account services and as the medium for new direct payment mechanisms which can be utilised between buyer and seller and financial institution and customer.

USING THE INTERNET FOR REMOTE ACCOUNT ACCESS

The Internet opens up some attractive and intriguing possibilities for remote account access, including the following:

- financial institutions which customers deal with only through communications networks and which may have no physical branches (cyberbanks);
- a full range of inquiry and transaction services 24 hours a day;
- customers easily able to access recent and historical transaction data (eg account activity in the last 2 hours or the last 12 months) at low cost;
- financial institutions located anywhere in the world, readily accessible to customers with an Internet connection located anywhere in the world, not necessarily subject to the regulatory regimes of the customer's jurisdiction;
- direct customer control of international movement of funds without the intermediation of financial institutions in the customer's jurisdiction;
- using stored value smart cards in card readers attached to customers' personal computers to transfer electronic value between cyberbank and smart card, thus making the customers' computer a private automatic teller machine.

Developments in Internet Remote Account Access

One of the first cyberbanks to establish itself was Security First Network Bank (SFNB) in the USA,[1] a subsidiary of a regional bank holding company. SFNB does not have a bricks and mortar branch for over the counter transactions. It commenced operations in October 1995 operating out of a single office in Kentucky. SFNB allows customers to open accounts by filling out an on-line application. If approved, customers are mailed a kit including customer ID and password. Using these, customers can review activity on all their accounts (updated daily), make transfers between these accounts and issue instructions to the bank to pay bills by electronic transfer or bank-issued cheques.

[1] www.sfnb.com.

At the time of writing,[2] Advance Bank and the Commonwealth Bank of Australia are the only Australian banks to have gone live with Internet remote access for transaction services.[3] Other Australian banks have promised to introduce Internet transaction services soon.

Taking Advance Bank as an example, to access Advance Bank's Internet banking service, customers must download application software from the Advance Bank site (including a security module) in order to configure the viewer on their Internet browser to show account details and transfer instructions. Customers are issued with a 16 digit Internet account access code and a 4 digit PIN. Once the correct code and PIN have been entered, customers can review account transactions, transfer funds between their own savings, cheque, credit card and home and personal loan accounts and pay bills to third parties (of the customer's choice, including other financial institutions). The application software is periodically updated and the new versions must be downloaded by customers. The software uses a virtual PIN pad for entering the PIN rather than the physical computer keyboard to avoid any keyboard monitoring virus that may be in the customer's computer.

Of course, a cyberbank offering remote account access need not be located in Australia, and it may not be a licensed bank or financial institution under Australian law. A computer operator and an internet connection are the essential elements for a cyberbank. Whether customers will use offshore cyberbanks will depend upon whether the customer trusts them to honour their obligations. If that trust can be established, depositing money in an offshore cyberbank may offer to retail and small business customers:

- significant tax and regulatory arbitrage advantages over deposits with Australian institutions:

- direct customer control over the placement and movement of offshore funds without the intermediation of Australian financial institutions.

These advantages are of concern to national tax authorities[4] and law enforcement[5] who fear tax evasion and money laundering activities which will escape the current reporting net that relies on the intermediation of Australian financial institutions in many funds transfers. Those fears are not without foundation. Some cyberbanks have set up in tax havens and bank secrecy jurisdictions.[6]

Withdrawals and Deposits with Cyberbanks

Currently in most applications of Internet remote access banking, deposits and withdrawals have to be made off-Net, using existing payment mechanisms such as cheques, cash or electronic funds transfer through the existing interbank payment and clearing systems. Eventually, personal computers or telephones equipped with smart card readers will turn those terminals into the equivalent of personal automatic teller machines by permitting the transfer of electronic value between the chip on the smart card and a bank via telephone lines or the Internet. The Mondex stored value smart card, in trial in the UK and elsewhere, but not yet in public trial in Australia,

[2] May 1997.

[3] See www.advance.com.au and www.commbank.com.au/netbank.

[4] The Australian Taxation Office is concerned that the use of electronic commerce over the Internet might erode Australia's revenue base. The ATO set up a task force in March 1996 using specialists to examine the technological, legal and financial aspects of the Internet as it affects taxation. It is to report by June 30 1997. A tax office web site has a FAQ link for questions about the taskforce: http://www.ato.gov.au/.

[5] See AUSTRAC, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board* November 1996.

[6] Eg The European Union Bank in Antigua (www.eubank.ag).

allows this transfer of value to and from smart cards through telephones and personal computers.[7] Other stored value smart card developers plan similar functionality.

But smart card readers require the acquisition by customers of new hardware. Other developers such as Digicash have sought to produce purely software-based payment solutions, accessible by ordinary PC equipment with an Internet connection. These software solutions involve new digital stores of value known as digital coins and digital cheques. These stores of value can be used for withdrawals and deposits from on-line financial institutions and can also be used for direct payments between buyers and sellers on the Internet. Direct Net payment mechanisms are considered further below.

Customer Confidence and Legal Issues in Internet Remote Account Access

Internet Banking Security Concerns

Customers are understandably concerned about the security of their accounts and transactions once Internet access is available. Most Internet banks seek to assuage customers' fears by providing and heavily advertising state of the art security systems and message encryption.

Advance Bank's network security is based on (1) a firewall between the bank's host computer and the Internet server and (2) encrypting all messages between the application software running on the customer's PC and the bank computers using public key cryptography (RSA and IDEA 2.2 with 128-bit session keys). The account access code and PIN are additional customer-controlled security measures. Public key encryption enables the use of digital signatures and certificates to ensure that payment messages are confidential and not tampered with and permits independent authentication of the sender by binding the message to the identity of the person holding the private key by which the message was signed.

For many customers, all the state of the art engineering and cryptography of these security systems will be but a sophisticated form of a "trust us" appeal, and most customers will be ill-equipped to evaluate the risks and security systems themselves. Financial institutions in some countries can make a second appeal for customer trust based on deposit insurance systems. In the case of US banks, the Federal Deposit Insurance Corporation protects deposits and effectively takes the risk of hacking up to $US100,000 (depending on circumstances). Australia has no form of public deposit insurance, so that argument is unavailable to Australian banks. Banks could themselves underwrite the risks – American Express has promised to compensate its US cardholders for any losses they incur through security breaches in Internet transactions using the Amex credit card. Astute customers might look to see how much the cyberbank trusts its own security by seeing how its terms and conditions allocate the risk of loss from unauthorised transactions on the cyberbank or the customer.

Cyberbank Creditworthiness Concerns

An even more fundamental issue is the creditworthiness and honesty of a cyberbank. A cyberbank may be no more than an operator with a computer and Internet connection, so commercial reputation and, perhaps, submission of the cyberbank to a known regulatory system, may be crucial to engender customer trust. Customer decisions to entrust their money to cyberbanks probably will depend upon the established reputation of the cyberbank, the amount involved and returns expected and available means of redress in the event of trouble (eg does the cyberbank have a physical presence and assets within the customer's jurisdiction or a jurisdiction where the customer's rights can be effectively vindicated?).

[7] http://www.mondex.com/mondex/home.htm.

Some Legal Issues in Remote Account Access Cyberbanking

Governing Law

The question of what system of law governs cyberbanking transactions is considered in more detail below. The following discussion of legal issues assumes that the law of an Australian jurisdiction governs the transactions.

Application of Finance Industry Codes of Conduct to Cyberbanking by Australian banks

(a) The Code of Banking Practice (and the equivalent Codes for Building Societies and Credit Unions) will apply to banking services provided by Australian banks to customers through the Internet. Notably, banks subject to the Code must disclose their terms and conditions, fees and charges and information on the operation of account operation and payment services to customers. The terms and conditions must be made available in writing. Variations to the terms and condition s must be provided in writing or in some cases by newspaper advertisement. Other information must be made available to the customer without limitation as to the medium.

(b) The EFT Code currently applies to "transactions intended to be initiated by an individual through an electronic terminal by the combined use of an EFT plastic card and a personal identification number (PIN)": clause 1.1.

Hence it does not cover remote account access transactions without cards such as telephone and Internet banking, nor transfers of digital coins or cheques. Many of the provisions of the EFT Code are adaptable to newer forms of remote account access such as telephone banking, PC banking and Internet banking. The report of a review of the EFT Code to consider making it technologically neutral and adapting it to other forms of electronic banking is long overdue and may be hastened as a result of the Wallis inquiry.

The EFT Code contains detailed provisions for allocation of loss arising from unauthorised transactions. Broadly, customers are liable for loss only if they are negligent with the PIN code or unreasonably delay in reporting loss or theft of the card or PIN. What loss allocation rules will apply to Internet banking? Some assurance that customers will face fair allocation of risks of unauthorised transactions and system or equipment malfunction is needed if customers are to be confident about entrusting their funds to these new systems. The two operational Internet bankers have taken different approaches. Advance Bank's terms involve a rather draconian imposition of liability of the customer in the case of unauthorised transactions.[8] However, the Commonwealth Bank has voluntarily adapted the EFT Code liability allocation provisions in their terms for telephone banking and Internet transaction banking.

Liability under the Trade Practices Act for Breach of Minimum Service Quality Warranties

Section 74 of the Act provides in slightly paraphrased form:

> In every contract for the supply by a corporation in the course of a business of services to a consumer, there is an implied warranty that:
>
> - the services will be rendered with due care and skill;

[8] Clause 23.6 provides: "We are not liable for any loss caused by unauthorised access or breach of security through Quicklink."

- material supplied in connection with those services will be reasonably fit for the purpose for which they are supplied;
- if the consumer makes known any particular purpose for which the services are desired, the services and materials supplied will be reasonably fit for that purpose (unless the consumer does not or should not reasonably rely on corporation's skill and judgment).

Possible applications of section 74 warranty to a supplier of electronic banking systems may include the provision of a reasonable level of

- availability of service and equipment
- maintenance of service and equipment
- security of transactions
- successful completion of transactions
- recovery of unsuccessful transactions

having regard to industry and technological standards, domestic and international.

A person acquires goods or services as a consumer if:

(a) the price does not exceed $40,000; or

(b) the goods or services are of a kind ordinarily acquired for personal domestic or household use or consumption.

Under section 68, any term of a contract that has the effect of excluding, restricting or modifying rights or liability under implied warranties is void. Under section 68A if the services are **not** of a kind ordinarily acquired for personal, domestic or household use or consumption, liability of the corporation may be limited to replacing the goods and resupplying the services or the cost of same. Internet customer banking transaction services arguably are or are becoming services of a kind ordinarily acquired for personal domestic or household use or consumption. Liability for breach of the implied warranties in respect of those services therefore may not be limited.

The Federal Court has held that if otherwise unqualified exclusion or limitation of liability clauses make only a casual nod in the direction of non-excludable rights under the Trade Practices Act, the overall impression may be that the unqualified exclusions apply and the corporation may be liable for misleading statements concerning customer rights under section 53(g).[9] Some providers of telephone and Internet banking services need to re-evaluate their current terms in the light of the Federal Court decisions.

Another possibly fertile area for claims about misleading and deceptive conduct is the area of representations about the level of security.

SECURITY, AUTHENTICATION AND MESSAGE INTEGRITY IN INTERNET ELECTRONIC COMMERCE

Before discussing specific Internet payment mechanisms, it is desirable to canvass issues of security, authentication and message integrity in more general terms, including a description of the most popular solution to these issues: asymmetric public key cryptography.

[9] *TPC v Radio World Pty Ltd.* (1989) ATPR para 40-973.

Security, authentication and message integrity are key concerns for all users of open network electronic commerce systems.

Security is the prevention of unauthorised sending, viewing or tampering with electronic messages or records.

Authentication is the process of assuring the recipient of an electronic message that it was sent by apparent sender. This is crucial in banking where the basic legal concept is that a customer's account cannot be debited without the customer's mandate. The cyberbank needs to be assured that the customer has indeed sent the electronic message authorizing a transaction on the account. Authentication links to the concept of **non-repudiation** which means that the apparent sender is legally bound by and is not able to disavow the electronic message.

Message integrity means that the message received is the in the same form as the message sent.

Security, authentication and message integrity are easier to ensure when banking transactions occur through proprietary networks such as the ATM and EFTPOS networks. Even in that context, arguments can and do occur about alleged unauthorised transactions because of system malfunctions and more often because the customer authentication system (a 4-6 digit personal identification number or PIN) is a relatively weak authentication method, liable to be guessed or surreptitiously observed and misused by a third party to perpetrate unauthorised transactions.

In open networks such as the Internet, there is an unknown and unknowable class of eavesdroppers and copiers who may be observing or recording messages. In open networks security much stronger than a PIN is required. The most common form of authentication used in open networks is an electronic signature based on a cryptographic key (or code). The sender of a message encrypts the message with a key and only someone who knows the relevant decoding key can decrypt and read the message. In this way encryption can keep the message confidential and provide a presumption of authentication that the message came from the purported sender if it is assumed that that person kept the encoding key secret.

A particular form of cryptography called asymmetric public key cryptography provides a stronger basis for authentication and message integrity as well as confidentiality. Public key cryptography is based on a pair of different keys, one private, the other public. A message encrypted with one of the keys can only be decrypted with the other key in the pair (hence asymmetric). The public key is made publicly available in a public key directory by a third party **certification authority** which will certify that the public key is paired with a private key belonging to a designated individual or organisation. The private key is kept secret by the entity to whom it belongs.

Confidentiality of a message can be ensured by encrypting it with the recipient's public key. Only the recipient who holds its private key can decrypt the message.

Authentication of a message can be ensured by the sender (say a customer) encrypting it with its private key. That message can only be decrypted using the customer's public key. The bank that receives the message purporting to come from the customer can check the public key directory, find the customer's public key and use the public key to decrypt the message. If it works, then there is a very high degree of assurance that the message was encrypted with the customer's private key and, if it is assumed that the customer has kept secure control over the private key, there is a high degree of assurance that the message was sent and authorised by the customer.

If authentication but not confidentiality is required for the message, then the body of the message can be sent unencrypted but the customer can "sign" the message by computing a unique hash value for the message, then encrypting the hash value with the customer's private key. The recipient bank can independently calculate the hash value of the message received, then decrypt the hash value calculated by the customer using the customer's public key. If the two hash values agree then the bank knows with a high degree of assurance:

- that the message was sent by the customer (establishing authentication); and

- that the message was not altered in transit, because such alteration would have changed the hash value – this provides an assurance of **message integrity**.

A message with a hash value encrypted with the sender's private key is called a digital signature.[10]

Digital signatures have been distinguished from electronic signatures as follows:

> "A **digital signature** can be defined to mean a transformation of a record using an asymmetric cryptosystem and a hash function such that a person having the initial record and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the initial record has been altered since the transformation was made. In other words, a digital signature is created by use of a public key system, but an electronic signature includes broadly any computer method ... Digital signatures are technology specific. Electronic signatures are technology neutral."[11]

Digital signatures require a Public Key Infrastructure (PKI) in which a trusted third party (certification authority) can link a particular public key to the identity of a person or organisation. Several overseas jurisdictions have legislated to establish a PKI and give legal effect to digital signatures. A proposal for such a framework in Australia has been made in Standards Australia, "Strategies for the Implementation of a Public Key Authentication Framework" (PKAF) in Australia (SAA MP75 – 1996). The Federal Government is developing a response to this report and the Victorian Government is considering measures to give effect to digital signatures.

A key issue in deciding to what extent persons should be legally bound by the content of electronic messages signed with their private key is the level of security attached to the medium on which their private key is stored. It may be stored on a computer hard disk protected by a 6-8 digit password or it may be on a smart card protected by a 4-6 digit PIN. In a chain of security measures, the weakest link determines the strength of the chain. In many PKI proposals, the use of a private key is given the same legal effect as a general power of attorney. Is it appropriate to bind key-holders in all cases to all uses of their private key if the key is only protected by physical possession and a PIN number or password? Or is it more appropriate to analogise the use of a private key which has relatively weak physical security to the use of an EFT debit card and PIN and therefore apply develop other loss allocation rules for unauthorised transactions, perhaps using the EFT Code of Conduct as a starting point? This is a difficult issue requiring much more thought than it has so far received.

DIRECT PAYMENT MECHANISMS ON THE INTERNET

Existing Internet Payment Mechanisms

Insecure Credit Card Transmission

Early payment models involved payment by credit card with card details being supplied by email or other means across the Net. Because the transmission of unencrypted data across the Net is not secure, credit card details could be stolen by interloper hackers. In practice, such interception is hit and miss and unlikely to be cost effective. More effective hacking involved penetrating Internet merchant's sites and stealing collections of card numbers stored there.

[10] A good explanation of these concepts can also be found in Tyree, *Digital Cash* (Butterworths 1997) chapter 2.

[11] Greenwood, D, "Electronic Signatures and Records: Legal and Policy and Technical Considerations": http://www.magnet.state.ma.us/itd/legal/e-sig.htm.

More secure card-based payment systems

There are two forms of these:

(a) ***Encrypting the sending (and storage) of card details across the Net to make payments***

For example, Visa and MasterCard have published a specification called Secure Electronic Transactions (SET) for encryption-protected use of credit cards and debit cards to make payments in Internet commerce. Other organisations (eg CyberCash) have also been working to develop secure encrypted credit card transactions on the Net.

(b) ***Avoiding transmitting or storing card details on the Net***

Instead a user's card details and identity are transmitted off-Net to an intermediary (effectively an aggregator of card claims) which issues a substitute password to the user. The password is linked in the intermediary's secure computer to the card details. The user sends the password across the Net to the seller, the seller immediately refers the password and purchase details to the intermediary which obtains an email verification of the purchase order from the cardholder and then confirms the sale to the seller. The intermediary aggregates the amounts on the cards of users for a period and then claims the bulk amounts from the card company as a merchant. The intermediary takes a cut from sellers and purchasers. (First Virtual operates by this system.)

New Internet Payment Mechanisms: Encrypted Software-Based Payment Systems ("Digital Money")

These are of two types:

Digital cash is electronic token money (ie electronic "coins" or "notes") issued by an electronic bank issuer in exchange for real world money and able to be transmitted by a purchaser to a seller and banked by the seller at an electronic bank. A digital coin is a packet of digitised data, electronically signed by the issuer (using encryption) and certifying that it is worth and redeemable for a certain amount of real world money. The coin may be sent over the Net from hard disk to hard disk and redeemed at the issuer. (Digicash's ecash, which Advance Bank will issue is based on this idea.) In current applications, a digital coin is issued as a pre-paid store of value (the pre-payment being the debiting of the customer's account). But it could be issued on credit.

A **digital cheque** is electronic notational money. It is a packet of digitised data, electronically signed by the customer (using encryption) which acts as electronic authorisation from the customer to an electronic bank to transfer electronic value (previously purchased with real world value) from the issuer's account to an identified beneficiary's account. (NetBill and the Financial Services Technology Consortium's E-check are based on this idea.) The electronic cheque is sent direct to the payee who will present it for collection directly or through the payee's financial institution.

There are no digital cheque systems operating in Australia at this time but we are soon to get digital coins.

One of the leading developers of electronic token money in the world is Digicash, whose product ecash (a digital coin product) has been widely licensed to financial institutions throughout the world, including Mark Twain Bank in the USA, Deutsche Bank in Germany, EU Net Bank in Finland, Bank Austria and Den Norske Bank in Norway. In October 1996, Advance Bank announced that it would issue digital coins denominated in Australian dollars using Digicash's ecash software. Advance Bank is expected to go live with this system in June or July 1997.

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

Digital money is pure information representing an obligation of a party to convert it into real value. As pure information it needs to be authenticated as having come from the person who purports to have sent it and to be resistant to tampering and counterfeiting. Digital signatures, using certificates based on public key/private key cryptography, as explained above are used to authenticate the issuer of the coin and to verify message integrity.

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

USER CONFIDENCE ISSUES IN INTERNET PAYMENT SYSTEMS

Risk of Counterfeiting Electronic Stores of Value

"Counterfeiting" – Allocation of loss in the event of obtaining counterfeit electronic value

Can electronic value be "counterfeited" ie can the record of value be increased without corresponding payment of "real" value?

Can this be detected? Can genuine value be distinguished from false value?

If so, can false value be traced through transactions to see in whose balance it ends up?

What are the legal consequences if electronic value on a electronic can be counterfeited and who bears the loss of a successful counterfeit?

I am not qualified to answer the technical questions. Cryptographic experts tell me that with an appropriate phalanx of security measures, kept under review and updated with developments in technology, it is extremely unlikely that false electronic value could be created and accepted by cyberbanks.

If, however, we assume the worst, what follows? If false electronic value cannot be distinguished from genuine electronic value, then all electronic value is potentially suspect and effectively devalued because the redemption obligations of the issuer may exceed the value of the collateral out of which the redemptions are to be made.

If false electronic value can be distinguished from real electronic value, then presumably the issuer would refuse to redeem false value unless it was a minimal amount. If that false value has passed through the hands of innocent third parties, would it be possible to unwind those transactions to trace the false electronic value back to the point of introduction into the system and fix the loss on the person who first held that false value? It may be theoretically possible in a fully accounted system but in the case of a fraud of significant size and penetration, probably not practicable. In practice, there seem to be three possibilities:

- leave the loss with those who held false value when the music stopped, if it is distinguishable from genuine;
- distribute the loss across the whole system if the issuer could cover it; or
- the insolvency of the issuer.

Insolvency of issuer – Allocation of loss in the event of issuer/redeemer of electronic value becoming insolvent

What are the consequences if the entity who has promised to meet the claim recorded on the electronic becomes insolvent?

Electronic value is a claim against the issuing or account-holding institution. Presumably ordinary insolvency laws apply to the allocation of losses if the institution becomes insolvent. If the issuer is overseas, a potentially complex cross-border insolvency ensues.

In Australia in the event of a bank insolvency, the Australian assets of the bank must be applied first to meet that bank's deposit liabilities in Australia.[12] Depositors at Australian banks in Australia get some preference as creditors from this provision in the event of bank collapse.

Is electronic money in an Australian customer's ecash safe held on the computer of the financial institution, not in a regular account, subject to this protection? Clearly not if the electronic issuer was not a bank. Arguably, even if the issuer were a bank, once the value leaves a regular account for the ecash safe it may not be a deposit liability, thus the preference provision is not triggered. The attitude of the Reserve Bank on this point will be crucial.

REGULATORY ISSUES IN CYBERBANKING

Licensing, Prudential Regulation and Deposit Insurance for Cyberbanks

It is not only traditional financial institutions which are getting into cyberbanking. Telstra has foreshadowed a secure payments system in which it appears Telstra will stand between banks and retail customers and merchants for processing secure Internet retail payments. Depending upon the precise nature of the services offered, such a service may amount to banking business and require financial system regulation.

Under the current Australian regulatory framework, a cyber-institution which takes deposits and makes loans would be conducting banking business and would require, in the case of:

- general banking business – a licence under Banking Act;
- specific banking business – to be registered under the Financial Corporations Act or under the AFIC legislation if a building society or credit union.

It is a major definitional issue whether the exchange of digital coins for currency is to be characterised as a deposit for this or other legal and regulatory purposes. If I withdrew all my money from my account at Advance Bank and turned it into digital coins residing in an ecash safe on Advance bank's computer, is that value still on deposit with or in an account with Advance bank? The Wallis Committee made some reference to these issues, requiring some degree of

[12] Banking Act 1959 (Cth) section16.

prudential regulation for issuers of stores of value.[13] The Bundesbank is procuring amendments to German banking law to restrict the issue of stored value cards and electronic coins to licensed credit institutions.

The treatment under Australian law of offshore account holding institutions or issuers of digital money is problematic and probably requires a multilateral international regulatory response.

Money-laundering – AUSTRAC/RBA Working Groups

The Financial Transaction Reports Act 1988 is currently based on reports by cash dealers of:

- significant cash transactions (ie physical transfer of notes or coins);
- suspicious transactions;
- international funds transfer transactions.

Amendments may be needed to go beyond physical cash transfer paradigm where it applies.

If cyberbanks and digital coin issuers are domestic, a possible regulatory response is to require them to be supervised financial institutions and report issuance and clearing/settlement of electronic value.

If they are international, there is a serious problem! Individual Internet funds transfers will not require financial institution intermediation, thus escaping the current reporting net. Australian issuing institutions will report international clearing and settlement of electronic value claims from foreign collecting institutions but this will only provide aggregate figures.

SOME LEGAL ISSUES IN CROSS-BORDER TRANSACTIONS

If an Internet banking service is to be offered to customers outside the home jurisdiction of the offering financial institution, a number of legal issues arising from the cross-border nature of the relationship and transactions need to carefully considered, as well as the practical issue of enforceability of a transaction against a counterparty in another jurisdiction. The legal issues include the following.

Governing Law of Contracts

The law that governs contracts formed by offer and acceptance over the Internet will be determined by the conflicts of law rules in the forum where suit is brought on that contract. Most Western jurisdictions recognise party autonomy in choice of law and will give effect to expressly agreed choice of governing law, subject to some exceptions. If the financial institution can include an express choice of law clause in the customer contract, that will usually bind the parties in suits in Western legal systems. Similarly, the financial institution could include an express choice of jurisdiction clause. Whether retail or small business customers will agree to the financial institution's choice of law and jurisdiction clauses is another question.

If there is no express choice of law clause, the conflicts rules of the forum where suit is brought determine the governing law. This will turn on a range of connecting factors to relevant jurisdictions, including the place where the contract is formed.

[13] See Recommendation 72 and accompanying text.

Regulatory Jurisdiction

Careful thought also needs to be given to:

1. the cyberbank's home jurisdiction regulatory authorities' attitudes regarding:

   (a) prudential and other requirements concerning offshore assets and liabilities generated through cyberbanking;

   (b) the application to cyberbanking transactions of financial reporting requirements concerning cross-border transactions for money-laundering and taxation purposes.

2. the application of the financial system regulatory laws, taxation laws and consumer protection laws (among others) of the home jurisdiction *and of those jurisdictions where the financial institution intends to solicit customers through its Internet banking services.*

The questions as to which governments can assert jurisdiction over cross-border cyberbanking transactions are extremely complex and are still being studied as part of our research project on Electronic transactions law. What follows is a preliminary skirmish at some of the issues.

The advertising or offer of goods or services (including securities) on the Internet may be accessible throughout the world. Does the mounting of an advertisement or offer or prospectus on a web site make the person who mounts that information subject to the regulatory laws of every jurisdiction where the information may be accessed, ie every jurisdiction in the world? Eg licensing laws and consumer protection laws.

The question must be answered having regard to three factors:

- whether the existing law catches such out-of-jurisdiction activity;
- the political likelihood of the existing law being amended to extend its jurisdictional reach (this would include an assessment of domestic constitutional limitations on the enactment of extraterritorial laws and international relations limitations on such enactment);
- the practicalities of enforcing an extraterritorial law.

1. The reach of the existing law:

   It is a question of interpretation whether particular laws in particular jurisdictions currently apply to:

   - offers mounted on websites out of that jurisdiction but accessible within that jurisdiction;
   - actions by a person in the jurisdiction in response to the web offer;
   - further actions taken by the out-of-jurisdiction offeror in response to actions by the person within the jurisdiction.

   A possible answer to some of these questions about the reach of current laws relies on the **push/pull theory** of Internet jurisdiction. If the foreign person uses the Internet to **push** information into the jurisdiction, eg by unsolicited email to persons within the jurisdiction, then that is akin to pushing paper or broadcast advertising into the jurisdiction and is more likely caught by laws prohibiting the doing of acts inside the jurisdiction.

   But if the information is simply mounted on a foreign website such that it needs to be **pulled** into the jurisdiction by an Internet browser operating from within the jurisdiction, arguably the foreign mounter of that information has facilitated someone in the jurisdiction pulling that information but has not done any act within the jurisdiction and can therefore escape existing laws if restricted to acts done in the jurisdiction.

2. Extension of current laws to cover foreign websites:

   Even if current laws do not cover foreign websites, local sovereigns may amend these laws seeking to regulate or prohibit these. Eg sites that contain pornographic material, gambling services, political material deemed unsuitable or prospectuses that have not been registered or banking services that have not been licensed by the local sovereign.

   Subject to domestic constitutional law limits, local sovereigns can enact laws having extra-territorial effect to do this (or criminalise the use of such websites by persons within the jurisdiction). Some US trial courts have upheld State statutes which criminalise the provision of certain information or services on out of State websites.

3. Finally, an eye then must be had to the practicalities of enforcement because even if the jurisdiction's statute makes the information or offer on the foreign website illegal, can that law in practice be enforced – can the out-of-jurisdiction offender be effectively stopped by legal process? Or can the actions of in-jurisdiction counterparties (investors/purchasers) be effectively deterred by legal process?

   This depends on whether the out-of-jurisdiction offender can be made subject to the jurisdiction's legal process, whether that judgment can be enforced and executed against their assets wherever they are located.

Considering this issue on a global scale, I feel considerable doubt about the capacity of one sovereign to effectively prohibit foreign websites of which it disapproves.

There is a possible draconian solution for draconian states – to control all Internet service providers and hence all Internet access within the jurisdiction and block undesirable sites. But that requires an ongoing audit of ever-changing and ever-moving sites, which will be the labor of Hercules and far from foolproof.

For states committed to freedom of speech and wide Internet commerce that is not an option. The best available route at the moment is co-operative action among national regulators, be they securities commissions, financial institutions supervisors or consumer protection agencies, according to agreed common policies. Participating regulators can act against website operators within the participating jurisdictions. This is not a perfect solution. There will be gaps in international regulatory co-operation. Small states will see an economic advantage in lesser or no regulation or lower taxes such as bank secrecy jurisdictions do now. Unless those states can be brought in line or effectively frozen out of international payments system, there will be gaps that can be exploited by money-launderers and organised crime among others. The solution is not perfect but it is probably the best we can do at the moment.

CONCLUSION

In the time available to me in the conference program, I have only been able to sketch a number of the issues in cyberbanking and analyse some of them. There are plenty of issues for lawyers, regulators and bankers to think about for some time to come.

Cyberbanking will likely grow as a domestic banking service in Australia. Probably, cross-border cyberbanking will develop also, although its future will depend upon the pricing and returns offered, on customer trust in the integrity of the foreign cyberbank and the enforceability of its obligations, and on the resolution of the legal, regulatory, tax and jurisdictional issues mentioned.

EXTRACT FROM ADVANCE BANK'S GENERAL TERMS AND CONDITIONS

27. TRADE PRACTICES ACT

27.1 Certain legislation, for instance the Trade Practices Act (the Act), has the effect of giving you rights which cannot be excluded, restricted, or modified by agreement. Nothing in this agreement has the effect of excluding, restricting or modifying such rights.

27.2 If you do not use your Account or Payment Service only for private or domestic use, then our liability is restricted, in accordance with section 68A of the Act, to:

(a) in the case of goods, the replacement or repair of the goods or the cost of replacing or repairing such goods; or

(b) in the case of services, re-supplying the services or the cost of re-supplying such services.