Liability Issues in Internet Banking In Malaysia

Gita Radhakrishna

Multimedia University, Melaka Campus, Faculty Of
Business And Law, Jalan Ayer Keroh Lama,
75450 Melaka, Malaysia
Email:- gita@mmu.edu.my

ABSTRACT:-

Electronic banking, particularly internet banking has revolutionized the banking industry making transactions faster and more convenient. But security issues present a pressing concern. Even with the best supervisory and security devices losses may occur. This paper examines the regulatory framework in Malaysia as set out by the Central bank, Bank Negara Malaysia and compares it to the United Kingdom and Australia. The focus is on civil liability issues in this area and in this context a landmark case in the United States of America with potential global impact is discussed.

LIABILITY ISSUES IN INTERNET BANKING

1. INTRODUCTION

Internet banking was first introduced in the United States of America (USA) in the early 1990s and it has since extended globally gradually. Internet banking is a product of e-commerce in the field of banking and financial services. It offers different online services like balance enquiry, requests for cheque books, recording stop-payment instructions, balance transfer instructions, account opening, settlement of online credit card transactions resulting from online shopping and other forms of traditional banking services. Mostly, these are traditional services offered through internet as a new delivery channel. But, in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and, hence, has compelled regulators world over to take note of this emerging channel.

2. LITERATURE REVIEW

The Reserve Bank of India's Report on Internet Banking (2001) outlines some of its distinctive features:

(i) It removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdictions. This has raised the question of jurisdiction of law and / or supervisory system to which such transactions should be subject,

(ii). It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges,

(iii) Security of banking transactions, validity of electronic contract, customers' privacy, etc., which have been traditional banking concerns have assumed different dimensions given that internet is a public domain, not subject to control by any single authority or group of users,

(iv). It poses a strategic risk of loss of business to those banks who do not respond in time, to this new technology, being the efficient and cost effective delivery mechanism of banking services,

(v). A new form of competition has emerged both from the existing players and new players in the market who are not strictly banks as several policy decisions have also been made.

The Basel Committee on Banking Supervision (2001) established the regulatory framework to govern internet banking services. The thrust of regulatory action has been to identify risks in broad terms and to ensure that banks have minimum systems in place to address the same and that such systems are reviewed on a continuous basis in keeping with changes in technology. The other aspect is to provide a conducive regulatory environment for orderly growth of such form of banking. As mentioned above the BCBS has been working to develop guiding principles for:-

(i) prudent risk management of e-banking activities
(ii) consideration of cross border issues
(iii) promoting international co-operation and
(iv) encouraging an facilitating supervisiory training programmes

The BCBS established the Electronic Banking Group (EBG) to address these issues These have adopted globally to facilitate international standards and confidence in banking.

According to A.K.Pennathur(2001) online banking is a potential minefield of legal issues. Legal risks may arise form violation of laws, rules and regulations ranging from basic issues of customer privacy and disclosure to money

laundering and liability concerns in online banking.
Anita Ramasastry (2005) questions whether banks have a legal duty to protect their internet banking customers personal computers. She expresses the view that customers should be solely responsible for the security of their personal computers whilst the banks liability should be limited to their own networks over which they have control
With respect to liability there is no international accord and these have been left to individual Central Banks and even to the individual banks themselves to formulate a policy. This paper compares the position in Malaysia with that in the United Kingdom and Australia which share a similar legal background being part of the English Commonwealth.

3. Regulation of Internet Banking

3.1 Malaysia

Banking and all banking and financial services in Malaysia is regulated by its Central Bank, Bank Negara Malaysia (BNM). Internet banking made was introduced in Malaysia in June 2000 when BNM allowed the local banks to offer internet banking services in Malaysia. In 2002 the facility was extended to foreign owned banks as well. As of Jan. 2008 there were 23 banks offering internet banking facilities in addition to their traditional services. BNM has provided. **' Minimum Guidelines on the Provision of Internet Banking Services by Licensed Banking Institutions' (MGIB) 2000** modeled after the BCBS recommendations. BNM defines ***internet banking*** as being 'products and services offered by licenced banking institutions on the internet through access devices, including personal computers and other intelligent devices'. ***Banking institutions*** are legal entities licensed under the **Banking and Financial Institutions Act** (**BAFIA) 1989.** The aim of the **MGIB** is to protect both consumers and the banks themselves from the risks associated with such banking. The BNM guidelines are systematically structured into 6 chapters dealing with the types of internet banking sites, oversight, risk management, security, consumer protection, compliance and other general requirements.

Prior to the offering of internet banking services, BNM requires banks to have a web page to educate their customers on the various issues including:-

(i) terms and conditions for the use of internet banking services,
(ii) the risks involved in using the internet banking, eg. risk of '***phishing***' where fraudsters copy the bank's website and set up a fake page that appears to be part of the bank's web site. A fake e-mail is then sent out with a link to this page which solicits the user's credit card data or password.
(iii) statement of liability. Customers should be fully aware of their rights and responsibilities and that they are responsible for their own actions. Banks will be absolved from liability in the case of disputed transactions arising from the customer's failure to adhere to these guidelines. In this context the guidelines specifically provide that " contractual arrangements for liability should provide for sharing of risks between the banking institution and the customers. Customers should not be liable for loss not attributable to or not contributed to by them" This is a highly contentious area as banks often contract out of their liability.
(iv) that maximum limits may be specified for fund transfers to limit their risks,
(v) advised to read the privacy policy statements prior to providing any personal information to any third party advertisers or hyper text web links,
(vi) educating customers on their role in maintaining security of banking information by not sharing IDs and passwords with any one and by regularly changing their passwords and remembering to sign-off.
(vii) notification of any variation in terms and conditions,
(viii) advise on contractual arrangements for liability arising from unauthorized or fraudulent transactions, mode of notification, and information relating to lodgment of complaints.
(ix) a *Client Charter on Internet Banking* stating the institutions policies, products and services and commitment to offering quality service.

Since its introduction in 2000 various online frauds and scams have emerged giving rise to grave concern. The table below shows general statistics for various online fraud including phishing compiled by Cyber Security Malaysia since 2006 which shows a worrying trend necessitating stringent supervision and clear guidelines on liability issues to assist innocent victims .

Fraud statistics (Cyber Security Malaysia)

Yr.	Jan.	Feb.	Mar.	Apr.	May	June
2006	9	23	22	32	31	26
2007	33	15	22	20	59	42
2008	22	33	33	37	57	112

Yr.	July	Aug.	Sept.	Oct.	Nov.	Dec.
2006	34	21	31	23	30	9

2007	31	18	30	23	35	36
2008	95	75	90			

3.2. United Kingdom

At present there is an absence of any legal framework laying down clear rules as to the apportionment of liability in the event of any disputed online transactions be it in the event of fraud or a systems failure or malfunction. In 1986 a "Banking Services: Law and Practice" Review Committee was set up which published its report in 1989. the Committee was particularly concerned with customer activated Electronic Fund Transfers (EFT) transactions. the Committee recommended the adoption of provisions similar to s**.83** and **s.84 Consumer Credit Act 1974** that a customer should be liable for losses incurred up to the point where the customer notifies the bank, subject to a financial limit. The bank would be liable for loss thereafter. Where gross negligence on the part of either party could be proved, then that party should be liable for the full amount of the loss. Three different approaches as taken by banks can be observed. Firstly terms similar to card transactions ie. where banks assume liability from the point of notification but with certain limits imposed on the customer, secondly, banks that assume the entire risk until and unless it can be proved that the customer acted fraudulently or negligently and thirdly where a bank excludes all liability in case of fraudulent transactions until they are notified and this has been found to be the most common approach adopted by UK banks. Although banks are governed by a Banking Code each bank may set its own terms and conditions on the matter and the customer has no choice but to abide by them or change the bank. **S. 2** of the new **Banking Code 2008 (**the **Code)** includes key commitments requiring banks to treat customers fairly. **S.12** of the **Code** gives customers the most up to date information on how to protect their accounts from fraud. Liability is outlined in **s.12.13:-**

Unless you have acted fraudulently or without reasonable care (for example by not following the advice in section 12.9), you will not be liable for losses caused by someone else which take place through your online banking service.

The burden is on the customer to take all reasonable precautions and show that all instructions given by the bank had been complied with. However there are still grey areas that need to be resolved.

3.3 Australia

The **Electronic Funds Transfer Code of Conduct (Revised 2002)** (the Code**)** operative since 1st. April 2002, provides best practices for consumer protection in a technology neutral form for users of electronic banking and payment products. The Code is voluntary but once adopted by a Bank it becomes contractually binding upon the banks and financial institutions. The Code sets out detailed rules regarding allocation of liability in cases of losses from unauthorized transactions. It takes a tiered approach to allocation of liability. **Clause 5.2** of the Code provides that the account holder will not be liable for losses that:-

(i) are caused by the fraudulent or negligent conduct of the employees or agents of the account institution;

(ii) relate to forged, faulty, expired or cancelled access methods;

(iii) occur before the device or code has been received by the user, where a code or device is required for the user to use the access method; or

(iv) caused by the same transaction being incorrectly debited more than once to the same account

Clause 5.3 also provides that the account holder will not be liable for losses resulting from unauthorized transactions that occur after the account holder has notified the financial institution of the loss or theft of any security code or device forming part of the access method. Financial institutions have a duty to provide an effective and convenient method of notification.

Clauses 5.5 and **5.6** set out circumstances where the account holder will be held responsible:-

(i) where the account institution can prove on a balance of probability that the user's fraud or the breaching of certain security requirements by the user contributed to the loss

(ii) where the account institution can prove on a balance of probability that the user contributed to the loss

by unreasonably delaying the notification of the loss, theft, misuse etc of the security code

(iii) where a secret code is required to perform the transaction and neither of the first two circumstances applies, the account holder is liable up to a limit of $150/- of the losses. This thus provides a no fault approach within limits.

In cases of systems failure **Clause 6.1** of the Code provides that the account institutions will be liable to their users for loss caused by the failure of an institution system or equipment to complete the transaction accepted by the institution in accordance with the user's instructions. Further by **6.2** an institution cannot deny its liability for a systems failure ie. it cannot contract out. Again **Clause 8.2** provides an institution cannot avoid its obligation by reason of the fact that they are party to a shared EFT system. This requires account institutions to secure back to back indemnity agreements.

The EFT Code is currently under review by Australian Securities and Investment Commission (ASIC). In so far as it relates to online banking it recommends that current provisions be retained and further seeks feedback on resolving the issue of mistaken payments From time to time, when making online payments, people accidentally pay the wrong person e.g. because they key in the wrong account number or because they have been given the wrong account number. There is currently a cause of action that allows people to recover payments made under a mistake of fact. The law on mistaken payments following decisions in **David Securities v Commonwealth Bank of Australia** and **Australia and New Zealand Banking Group Ltd v Westpac Banking Corporation** maybe summarized as follows:

- a mistaken payment is recoverable since the recipient is unjustly enriched
- in order to establish a prima facie right to recovery, the plaintiff must show that the payment was made because of a mistake
- it is then up to the defendant to establish reasons why the payment should not be returned.

Applying this law to the case of an electronic payment, a payment has been made under a mistake of fact to a person who would not have been paid but for the mistake. As a consequence, the payer has a prima facie right of recovery. The onus is then on the defendant to show why the payment should not be returned. The procedure for recovery is nevertheless onerous. While the law in this area is not settled, the proposals seek to offer the consumers protection benefits that go beyond the protections afforded by law and providing for a higher standard of conduct than required by law . It is also noted that any protection offered to bona fide mistakes may make the system more open to abuse and fraud by account holders who collude with each other, or where a single person opens two accounts using false identities.

4.BANKERS LIABILITY

This paper examines the issue of apportionment of liability in internet banking between the banks and the customers, primarily where customers suffer losses due to fraud committed by third parties and losses caused by systems failure or malfunction. Liability issues arising from disputed online transactions in internet banking may be classified into 3 broad categories namely:-

(i) **Human error either on the part of the Customer or the bank**. Here the concept of mandate is fundamental to the legal obligations of the bank to its customer. With certain exceptions a bank must follow its customer's instructions as to payment of funds out of the customer's account. These include who is authorised to operate the account. In the case of joint accounts, it is operating instructions will stipulate 'either one to sign' or 'both to sign' – the latter signifying that two signatures are required on cheques, withdrawal slips or other withdrawal instructions, such as redraw instructions for a home loan. Likewise the operating instructions for business accounts will include authorised signatories and whether one or, more usually, are required to authorise transactions.

(ii) **Technical malfunction or a system failure** be it within the control of the bank or outside the control of the bank. Execution of the customer's order though correct in all respects is delayed by the bank.

(iii) Fraud, either where the customer correctly issues an order but the transfer proves to be irregular, either in terms of amount or

identity of transferee due to fraud on the part of a a third party who uses the customer's means of access to make a transfer. A genuine unauthorized transaction due to fraud profits a third party and leaves a loss to be distributed between two relatively innocent parties, the bank and the account holder.

In any event these disputed online transactions may cause considerable damage and loss to the customer. However most banks have a disclaimer of liability clause along the following lines:-

" the bank and its partners shall in no event be liable for any loss and damages howsoever arising whether in contract, tort, negligence, strict liability or other contract basis, including without limitation, direct or indirect, special incidental, consequential or punitive damages or loss of profits or savings arising in connection with your access or use or the liability to access or use this website, reliance on the information contained in the website, any technical, hardware and software failure of any kind, the interruption, error, omission, delay in operation, computer viruses, or otherwise."

Thus the terms and conditions offered by the majority of banks are lop sided without a fair apportionment of liability between the bank and the customer. General contractual principles in respect of exclusion clauses require:-

- Clear words to be used to excuse a serious breach or negligence
- Should be brought to the attention of the contracting party before or during the contract
- must be sufficient

The ***contra proferentum*** rule of construction stipulates that in the event of any doubt as to the meaning and scope of the excluding or limiting terms, the ambiguity should be resolved against the party who inserted it and seeks to rely on it. However A party who signs a written contract is bound by the terms contained therein, 'whether he has read the document or not'. The law on unfair contract terms and the issue of the relative bargaining strengths of parties in standard form contracts leaves much to be desired.

In a recent interesting development in the United States, Joe Lopez, a Miami businessman who regularly conducted business over the internet, sued Bank of America at the Miami Circuit Court for negligence and breach of contract for failing to provide protection for online banking risks that the bank was aware of. On 6th. April 2004, his computer system was hacked into and US$90,348.65 was wired from his account at Bank of America Direct, its online portal, by Latvian cyber criminals, to Parex Bank, a bank in Riga, Latvia without his approval. About US$20,000 of the money was withdrawn before the account was frozen by the Latvian bank. A subsequent Secret Service investigation requested by the bank detected the presence of the *'coreflood keylogging Trojan'* on his computer. Lopez claimed that Bank of America had knowledge of the Trojan horse virus known for infiltrating and compromising security systems and enabling unauthorized access to infected computers, and therefore the bank had a responsibility to inform its customers of the virus. Further the bank should have been alerted when the transfer of such a large sum to Latvia was initiated. Latvia, along with Russia, Eastern Europe, and the other Baltic states is known for having a high level of cyber-criminal activity and thus a large monetary transfer to that part of the world should have been questioned by the bank. To make matters worse the bank failed to act upon being notified within minutes of the unauthorised transaction and refused to assist in liasing with the Latvian bank to freeze the monies or release the balance to Lopez. It was only in July 2004, that the bank sent a letter to its users alerting them to a new "dual administration" feature requiring the approval of at least two individuals to execute a funds transfer. The letter also recommended that clients install antivirus software. Bank of America denied liability for the loss since its systems were not hacked into and all appropriate measures were taken to complete the transfer. This action which which could have become a test case for determining bank liability in phishing frauds was however typically settled by Bank of America sometime in September 2005, the terms of settlement being naturally confidential. Thus a case which had potentially far reaching global impact ended prophetically as banks shy away from any adverse publicity.

5. Conclusion and recommendations

The liability issue thus remains very much open to be negotiated on a case by case basis between parties. Whilst banks may shy away from adverse publicity and be unwilling to risk litigation, more specific guidelines need to be formulated and an international accord reached for more equitable terms in the contractual relationship between the banks and their customers. In this respect the Australian Code although voluntary, is comparatively a first, and a very commendable effort in offering

reasonable equitable solutions which Malaysia would do well to incorporate.

Other possible remedial measures that could be adopted by financial institutions would be to:-

- **set transactional limits and verification of transactions**. Currently certain banks study their customers' credit card spending patterns and upon spotting any exceptional or suspicious transaction verify with the customer via telephone. This could be extended to online transactions as well. Certain limits could be set for online transactions beyond which, banks should immediately seek verification by calling the customers to confirm the authenticity of the transaction so as to avoid disputes and pre-empt opportunities for fraud.
- **Constant improvement of security features and continuous customer education.** Technology is constantly advancing and banks being better placed than individuals need to keep abreast of the latest security systems in the battle against technology based frauds. Customers should in turn be educated on the necessary security systems to have in place on their part.

- **Insurance** In addition to constant upgrading of security features and on going customers education banks should consider offering an additional layer of security in the form of insurance at no additional charge to the customers. Currently banks do offer accident protection policies and life insurance pegged to fixed deposit accounts as incentives to customers to bank with them. This same incentive could be extended to offering insurance against fraud in internet banking on a no fault basis. It would require negotiating with the insurance industry and would certainly give banks a competitive edge and bolster public confidence

- **Victim Assistance Services** providing clear methods for notification of any unauthorized transaction and immediate incident response to minimize the loss. Further assistance could also be extended to helping the victim lodge a police report
- **Independent Panel for Complaints** appointed by Central Banks to hear customer complaints. Panel members should be drawn from industry and from the professional sector such as IT, accounting and law to serve as a mediation board.

In conclusion, it is submitted that liability issues in internet banking have to be addressed on a concerted basis and an international accord achieved in order to protect users and instill confidence in the system.

REFERENCES

1. Abu Bakar Munir:- "Internet Banking Law and Practice

2. ABIO Special Bulletin on Electronic Commerce: Emerging Issues in Electronic Banking Disputes Bulletin 35; Available online:- [Visited on 10.5.2008] http://www.abio.org.au/ABIOWebSite.nsf/3f51d54074f36f08ca256bce00094be3/OpenDocument

3. Ahmad Azzouni :- " Internet Bnking and Law: A critical Ezamination of the Legal Controls over Internet banking in the UK" [2003] J.I.B.L.R 351 -360

4. AK Pennathur:- "*Clicks and Bricks":e-Risk Management for Banks in the Age of the Internet.*Journal of Banking and Finance 25(2001) 2103 – 2123. Available online:- http://userweb.port.ac.uk/~samieis/ebanking/articles/e-Risk%20Management%20for%20banks%20in%20the%20age%20of%20the%20Internet.pdf

5. Alan Tyree, 'Mistaken internet banking', March 2003, Available online:- http://austlii.edu.au/~alan/mistaken-epayments.html

6. Anita Ramasastry:- " *Do Banks have a Legal Duty to Notify Customers about Specific Computer Viruses?"* Available online:- http://writ.lp.findlaw.com/ramasastry/20050210.html

7. Banking Code 2008(UK) Available online:- http://www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf

8. Basel Committee on Banking Supervison "*Risk Management Principles for Electronic Banking*" (May 2001) Available online:- http://www.occ.treas.gov/ftp/release/2001-42a.pdf

9. Claessens Stijn, Glaessner Thomas and Klingebiel Daniela:- '*E- Finance in Emerging Markets: Is Leapfrogging Possible?'* Financial Sector Discussion Paper No.7 The World Bank June 2001,

10. Cyber Security Malaysia statistics on spam & fraud. Available online tp://www.mycert.org.my/en/resources/fraud/main/main/detail/514/index.html

11. Electronic Funds Transfer Code of Conduct (revised, 2002) Available online:- http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/eft_code.pdf/$file/eft_code.pdf

12. Review of Electronic Funds Transfer Code of Conduct by the Australian Securities and Investment Commission (ASIC) 2007/08. Consultation Paper 90 released on 3 Oct. 2008. Available online:- http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf/$file/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf

13. Finextra, 7th. February 2005:- '*Bank of America faces landmark online fraud case'*Available online:- http://www.finextra.com/fullstory.asp?id=13194 Also at :- http://www.accountingweb.com/cgi-bin/

14. Furst Karen, Lang William W., and Nolle Daniel E.:- ' *Internet Banking: Developments and Prospects'* (April 2002). Available online:- http://www.occ.treas.gov/netbank/ebankingdpapr02.pdf

15. Maybank2U.com Internet Banking Terms and Conditions. Available online:- http://www.maybank2u.com.my/bottom_nav/terms/

16. Minimum Guidelines on the Provision of Internet Banking Services by Licensed Banking Institutions

17. Reserve Bank of India:-'*Report on Internet Banking',* Avaialble online*:-* http://www.rbi.org.in

18. Saleh M Nsouli and Andrea Schaechtre:- '*Challenges of the e-banking Revolution'* Avaialble online*:-* http://www.bis.org/publ. [visited on 10.5. 2008]

CASES

1. Australia and New Zealand Banking Group Ltd v Westpac Banking Corporation(1992) 175 CLR 353
2. David Securities v Commonwealth Bank of Australia (1988) 164 CLR 662
3. L'Estrange v Graucob [1934] 2 KB 394 ;

4. Olley v Marlborough Court Ltd [1949] 1 KB 532 CA

5. Thornton v Shoe Parking Ltd [1971] 2 QB 163 CA

6. Alho Inc. v Bank of America (2005) Miami Circuit Court (unreported)