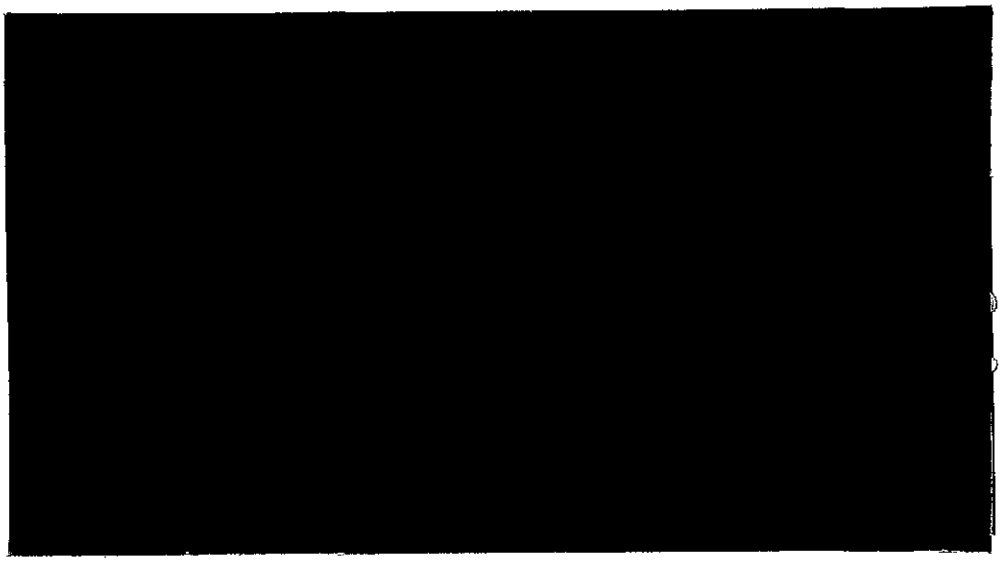
XXXII ANNUAL MONETARY STUDIES CONFERENCE



KINGSTON, JAMAICA

30 OCTOBER - 02 NOVEMBER 2000

TECHNOLOGICAL CHANGE AND RISK MANAGEMENT: BANKING INSTITUTIONS IN THE 21ST CENTURY

Jessel Subero
Research Assistant
Caribbean Centre for Monetary Studies

TECHNOLOGICAL CHANGE
AND
RISK MANAGEMENT:
BANKING INSTITUTIONS IN THE 21ST CENTURY

Abstract

The promises of technology in the 21st century holds unheralded prospects for the banking industry. The impact of technological integration on financial institutions from the viewpoint of risk management needs to be charted and properly assessed. This is especially true given the rapidity of technological change in the face of the globalization phenomenon. This paper seeks to examine the possible effects that electronic banking systems may have on banking institutions from a risk management viewpoint and to highlight some salient issues that confront regulators in this new dynamic.

INTRODUCTION

Rapid technological development is one of the major factors driving change in the banking industry globally. Technology has enabled the transformation of the industry, allowing for the development of new products and services, improvements in the efficiency of operations, and the electronic delivery of traditional products and services through open systems such as the Internet.

The continued development of the Caribbean financial services sector will be based to a significant extent, on the ability of regional institutions to keep abreast with, and harness, the benefits of information technology. As a wider use is made of technology, proper management of the risks in information technology will assume critical importance to financial sector operation and stability.

The focus of this paper will be concentrated on electronic banking issues and the impact that they are likely to have on risk management by financial institutions. This is indeed a timely topic as we are witnessing the phenomenal growth of electronic banking in the Caribbean. In Trinidad and Tobago alone, the volume of EFTPOS transactions has grown from 26,323 transactions in 1996 to 3,157,207 transactions by 1999, an increase of over 11000%, in just 4 years. The number of bankcards with Credit and Debit functions issued locally grew from 160,290 in 1997 to reach 511,901 by 1999, an increase of 220% in 2 years (See Appendix Table 1). Perhaps, most significantly, these volumes were achieved on a constant base of six commercial banks operating in the country over the period 1997 to 1999. Judging from the Trinidad and Tobago experience, it is obvious therefore that electronic banking is increasingly becoming an integral part of the financial landscape of the region. In the circumstances therefore an early examination of the risks entailed in these strategies is warranted and timely.

We shall begin by defining what is meant by "risk management" and examine its importance generally to financial institutions. The defining characteristics of electronic

banking is then examined, and a study of the various types of electronic banking strategies implemented by banks undertaken. Electronic banking brings about unique risks to financial institutions, and these are discussed in the terms of how they redefine the traditional risks that banking entities face. The special issues that these risks will raise for banking supervisors and regulators are then discussed as a means of provoking policy prescriptions for the emerging dynamic. Although no specific policy or legislative proposals are advanced, it is hoped that this paper will serve as a foundation to formulation of these initiatives.

RISK MANAGEMENT

In discussing the challenges faced by financial institutions in managing risk, we clearly have to define what we mean by "risk". For the purposes of this paper, we adopt the definition that risk is the possibility of experiencing a loss. Risk can also be described as being the reverse side of opportunity and reward. The roots of financial risk to industry have traditionally been linked to the performance of the economy, the trend in prices, market dynamics and other factors labeled as noise i.e. unpredictable events. The impact of technology on the banking sector has added a new dimension to the roots of risk for the industry.

Meyer (2000) in his paper "Issues in Financial Modernization" notes that the impact of technology on banking institutions, from a risk management perspective, as coming in two dimensions. Firstly, the rise in technological capability has enabled banking institutions to offer a new range of products and services. Secondly, the rise in computing power has enabled the quantification of risk. Thus financial institutions are now able to monitor and track all of the risks they face, with a degree of exactness and precision, which was hitherto impossible. The evolution of technology has therefore expanded the scope of risks faced by financial institutions, revolutionizing the ways these institutions undertake risks, whilst at the same time improving their capability to quantify, monitor and manage the said risks.

A key function of commercial banks is the management risk. Santomero (1997) notes that in the process of providing financial services, all financial intermediaries, assume a level of risk from or on behalf of their customers, and extract a fee or risk premium for doing so. It is precisely because of their expertise in managing risk, that market participants seek the services of financial institutions. How these risks will change over time, due to technological development is what we will examine, with specific reference to electronic banking strategies.

Risk Management can be described as being the art and science of mitigating risk factors. Oldfield and Santomero (1997) argue that the risks facing all financial institutions can be segmented into three separable types, from a management perspective. These are:

1. risks that can be eliminated or avoided by simple business practices
2. risks that can be transferred to other participants
3. risks that can be actively managed at the firm level.

The technological risk associated with electronic banking, I argue, falls into the third category. This is because the risks inherent in an electronic banking strategy are central to the bank's business purpose and must therefore be absorbed by the firm. The risks posed by this business strategy are clearly dependent on how the strategy is implemented at the level of the firm. Given that this is true, the risk of the strategy is absorbed by the firm, and the risk mitigation techniques required to be implemented therefore need to be effectively managed at the level of the firm.

THE ELECTRONIC BANKING ENVIRONMENT

The Basle Committee for Banking Supervision[1] defines Electronic Banking to be "the provision of retail and small value banking products and services through electronic channels". It includes electronic payment products and services in addition to activities such as the provision of financial information and account management activities.

Global Banking institutions have aggressively adopted technological developments to enhance their delivery mechanisms and to provide new products and services. The United States Federal Deposit Insurance Corporation (FDIC hereafter) attributes the growing importance of electronic systems to banking institutions to the following factors :

1. increasing competition from non-bank and non-traditional service providers for example mutual fund companies, telecommunication companies etc.;
2. increasing demands for more efficient and convenient capabilities by consumer;
3. the widening cost and delivery capabilities between electronic and traditional delivery channels.

The entering into a comprehensive electronic banking programme however is not without risks to the entity in question, and the mitigation of these "electronic" risks needs to be fully incorporated into the bank's risk management program.

A proper understanding of the electronic banking environment is essential for regulators and supervisors to grasp the risks inherent in such strategies being undertaken by banks. The electronic banking environment is generally thought of as being segmented into three basic lines. The classification used by the United States Federal Deposit Insurance Corporation and The United States Comptroller of the Currency follows the line of :

[1] Risk Management for Electronic Banking and Electronic Money Activities. March 1998

1. **Informational electronic banking systems.** This is typified by the bank hosting marketing information about its products and services on a stand-alone server (website). The risk in this type of framework is relatively low as there is no pathway from the stand-alone server into the bank's internal network. While the risk of penetration into the bank's network are low, there is the risk that alterations may be made to the content posted on the website. Controls are

therefore required in order to prevent unauthorised access of the information content of the site.

2. **Communicative electronic banking systems.** This system allows for data and information flows between the bank and its clientele. Communicative systems typically allow for account enquires, loan applications, electronic mail and static file updates (example name and address changes). It also includes systems in which data or files may be uploaded and downloaded between users, and the financial institution's proprietary databases and networks. Because these systems have pathways into the bank's internal networks, they create a higher risk profile for the entity. Controls are therefore needed to limit, prevent and to monitor access into the bank's internal networks and computer systems.
3. **Transactional Electronic Banking systems.** This type of system allows customers to execute traditional banking transactions electronically. Transactions generally include bill payment, transfer of funds, and balance inquiries etc. This is the highest risk architecture, as a links typically exists between the server and the bank's internal network. Strong controls are therefore a feature of this type of electronic system.

RISKS IN AN ELECTRONIC BANKING ENVIRONMENT

The advent of computer technology has redefined the nature and the scope of risks that financial institutions now face. As economic agents, we all operate in an uncertain environment. The concepts of risk and risk management therefore ought not to be external to our daily activities.

Generically, we can describe many different types of risks: credit risk, market risk, liquidity risk, political risk, legal risk, reputational risk, systemic risks and operating risk, amongst others. What is of concern to us as policy-makers is the way these traditional risks will be re-defined in an electronic banking environment. Using the major generic risk categories often associated with banking entities, we highlight some of the pertinent

transformation effects that an electronic banking strategy is expected to have on bank risk.

Credit risk is defined as being the risk of a debtor's failure to meet the terms of any contract, or otherwise perform as agreed. The offering of banking services via electronic mechanisms poses unique risks, because of the inability of the firm to interview and judge their clients on a personal basis. Other legal and logistical issues such as the verification of collateral, finalization of security agreements, affects the firm's overall risk profile. The new range of financial instruments made possible by Internet Technology therefore widens and deepens the levels of risk to which financial services providers are now subject. Banks and other entities providing these services via an electronic medium do so in a more risky environment and further account must be taken of this fact.

Interest rate risk is the risk arising from movements in interest rates. With an electronic banking strategy, banks are now able to engage in loans, attract deposits and engage in other transactions from a larger pool of customers. The need to maintain appropriate asset/liability management systems and the ability to react quickly to changing market conditions is now more crucial, as larger numbers of customers are now primarily seeking the best market rates and behave accordingly.

Liquidity risk is the risk arising from a bank's inability to meet its obligations when they become due, without incurring unacceptable losses. It generally arises from the inability to manage unplanned changes in funding sources, or the failure to recognize changes in market conditions, that affect the ability of the bank to liquidate assets quickly with minimal losses in value. Electronic banking can increase deposit volatility because there are some customers who maintain accounts purely on the basis of rates or terms. Increased monitoring of liquidity and changes in deposits and loans therefore may be warranted based on the volume of electronic transactions.

Transaction risk is the risk arising from fraud, error, the inability to deliver products and services, or to manage information flows. A high level of transaction risk exists with electronic products, especially those which are not adequately planned, implemented, and monitored. The delivery of accurate, timely and reliable services which meet the customer expectations is key, as customers are not likely to tolerate errors and omissions made with transactions over the web. Consequently, strong internal controls are required. These controls must be designed to provide not only accurate and efficient transactions, but also to be resistant to attacks and intrusion attempts from internal and external sources. Business resumption and contingency planning are also necessary to ensure that firms can conduct business in adverse circumstances.

With the banking industry now able to offer all of their traditional services over the web, there is concern that this type of service poses substantial **reputation risk** i.e. the risk arising from negative public opinion or declining customer confidence. The reputational risks posed include the risks associated with the improper disclosure of information; errors in processing, security breaches, fraud, and the interruption caused by hardware and software failures. These all have the potential to impact adversely, the reputation of the entities offering electronic banking services and ultimately the overall financial sector. Banks therefore must exercise an abundance of caution in dealing with customers through electronic media, ensuring that they are capable of delivering on marketing claims and providing accurate and timely services.

Strategy risk arises from the improper implementation of decisions or the lack of responsiveness to industry changes. The increased competition in the electronic banking arena has led to the widening of strategy risk. This has the potential of bringing about the problems of excess capacity and unsustainable cost structures in the industry, as institutions often predicate there electronic banking strategies on the same market segments. Banks also face the risk that the electronic product and services they seek to market may either be unacceptable to customers or could quickly become obsolete. Before introducing an electronic product, banks must consider whether the product and

technology are consistent with the tangible objectives of their strategic plan. The focus must therefore be on ensuring that the electronic banking plan is consistent with overall business objectives of the bank, and is within the firm's tolerance for risk.

Legal risk to the firm is also amplified by an electronic banking strategy as there is increasing uncertainty as to the legislation governing electronic banking issues such as validity and proof of transactions, and liability in the case of systems failure.

An increased reliance on electronic and computer systems to carry out banking activities also exposes the entity to heightened **operational risk**. Firms must take account of their vulnerability to computer malfunctions and break downs, and have proper contingency plans in place to treat with such problems. Risks arising from the lack of staff expertise, inadequate software and hardware controls, and problems resulting from shared networks with other institutional operators, all therefore increase the level of operational risk in a electronic banking environment.

Electronic banking activity also has an effect on **systemic risk**. This is especially true if many market participants utilize the same or similar software and hardware for running their electronic banking operations, as this subjects them to the same types of IT related problems and issues. Additionally, the outsourcing of operational functions such as payments processing will lead to the concentration of operational risk amongst all parties within the system.

RISK MANAGEMENT AND THE ROLE OF THE SUPERVISORY AUTHORITY

It is obvious from the above that the utilization of technology in the banking industry has created new regulatory and operational issues not only for bankers themselves, but also for supervisors in their role of guardian to the banking sector. Supervisors regulate risk for a number of reasons including:

1. to ensure the stability of the financial system;
2. to protect the safety and soundness of the banking system (capital adequacy);

3. to avoid the moral hazard problems that the existence of deposit insurance and the lender of last resort may create.

Whilst the over-riding risk factors facing banking institutions still have there basis in credit and market risk, operational risks are increasingly taking on a new and growing dimension because of technology. Banking supervisors and regulators now have to be extremely conversant with technological changes as they occur within the industry, and more importantly, need to be cognizant of the technology induced risks to the sector as a whole.

The risk management process should take account of, and encompass, all of the significant operational, legal, strategic, reputational and systemic risk areas identified above. A comprehensive review of the tools and assessment procedures used by regulators needs to be constantly undertaken, in order to equip the supervisors, to deal with the ensuing impact of technology. The emphasis of these general guidelines is on ensuring that banks have proper internal control procedures, to deal with the changing effects that technology will have on the banking industry. According to the Basle Committee Operational Risk Management Report of September 1998, most bankers expressed a preference for supervisors (and regulators) to focus on the qualitative improvement of technological risk management. Most bankers agreed with the premise that the process was not sufficiently developed for regulators to specify particular measurement methodologies or quantitative limits on the risks posed by technology.

In its publication "The Effect of Technology on The EU Banking Systems" of July 1999, The European Central Bank has adopted this qualitative approach where it states that "guidelines have to be put in place to ensure that banks:

- have an efficient management information system to handle the increasingly complicated business operations and environment;
- have policies and procedures in respect of the identification, assessment and controlling of the IT related operational risks, including the security aspects;

- have adequate control over outsourced IT-software development or functions of IT departments' activities, including the responsibility and accountability of external service providers, namely liability may arise if the products are not error free and banks themselves could be held liable for their customers;
- do not outsource the management of risks, since the ultimate risk management responsibility should always lie with the banks themselves."

CARIBBEAN REGULATORY ISSUES

Mitnick (1980) defines regulation as the public administrative policing of a private activity with respect to a rule prescribed in the public interest. Its purpose according to the Bank of England (1992) is to prevent systemic failure. Williams (1996) describes commercial bank regulation as being of three types: structural, monetary and prudential. Structural regulation, with which we are most concerned, refers to the limits placed on the activities of commercial banks, and determines the activities in which they may become involved and those from which they are debarred. Revell (1980) also describes structural regulation as setting the general parameters of the banking system, and as setting the context in which both prudential and monetary regulation operate.

The development of the banking sector that will arise out of the electronic banking phenomenon will bring to the fore a number of regulatory and supervisory issues for the Caribbean. Some of these issues referred to above include banks engaging in the geographic expansion and diversification of their markets, non-banking entities expanding their offering of traditional banking products, and institutions offering new services and instruments in banking. Spong (1994) details the task for regulators in this new dynamic, to be the establishment of a regulatory system that can accommodate these changes, while continuing to promote the regulatory objectives of depositor and consumer protection, monetary stability, and banking efficiency and competition. He identifies technological innovation as being one of several major factors that will affect the financial system in the future and thus inform regulatory changes.

Spong (1994) also identifies the continuing development of electronic banking and the growth of new banking products and services as two key examples of how technology is changing the banking system. He argues that by increasing the speed of transactions, creating new competitors and services, and altering banking bank operations and support functions, electronic banking is leading to many significant changes in our deposit and payments system. These developments will, amongst other things, enable customers to shift funds more readily between bank accounts, liquid investments, and other holdings; allow banks to offer a variety of innovative services such as derivative instruments; and facilitate the creation of new products and the entry into new markets.

Perhaps the most pressing of these issues facing us in the Caribbean is the regulation of "non-bank" entities that participate in banking activities. The ability of non-banking entities to offer banking services and instruments is enhanced with the growing acceptance of the Internet as a banking medium. The increasing pace of change in the financial services industry due to technological innovation, has led to pressure being put on the regulators to distinguish amongst different types of institutions. Meyer (2000) calls the existing prohibitions between banking and insurance anachronistic. Technological change, he argues, has simply undermined the traditional distinctions among financial products and services. As a practical matter, financial conglomerates may seek to structure their transactive flows in a manner to minimize the oversight of regulators. This can ultimately lead to regulatory arbitrage, unfair competition and market inefficiencies.

The monitoring of the cross-border activities of entities who offer services through the use of such portals as the Internet is another area of concern. The relative ease with which Internet based entities such as Wingspanbank.com and E-trade can penetrate our financial sector and offer banking and brokerage services in the Caribbean is known certainly in Trinidad and Tobago, where accountholders already exist. The lack of regulatory control and oversight of these institutions is a critical issue and undermines the reasons behind the regulation of the domestic market. The threat to depositor's interests and the possibility of capital migration are key issues of concern.

Supervisory authorities also need to concern themselves with the increasingly globalized state of the market for financial services brought about by technology. In this new financial landscape, the risks of contagion and its effects on the good order and functioning of domestic financial systems become of paramount concern. With the offering of unregulated financial services by external parties, the vulnerability of the domestic financial system is increased and this must be of strategic concern to Central Bankers.

Another issue will be the raising of the bar of public confidence in electronic banking services offered by entities, in light of the potential for fraud in electronic systems, especially during their developing stages, as now seen in the Caribbean. This can best be achieved through the standardization of encryption techniques, digital signature and other such electronic authorization procedures. National legislation dealing with the issue of computer misuse for fraud and criminal activity will also be of importance in boosting public confidence in the electronic banking framework going forward.

CONCLUSION

Technological innovations have increasingly impacted upon the nature of the financial services industry causing it to redefined itself. As the nature of the industry changes, so do the risks that businesses face. Electronic banking, it is clearly seen, is the future for the banking industry, and it presents unique opportunities and challenges. The unique characteristics of electronic services delivery, however, result in new dimensions of traditional risk. Consequently, both bankers and regulators need a series of new tools to address and manage these concerns. Governmental policy makers also need to have an ongoing understanding of the issues provoked by technological change to guide and direct overall policy and legislative initiatives.

This paper highlighted some of the salient risk management issues involved in the onset of an electronic initiative in the financial sector. It forms part of a larger work in progress

on the effects of electronic banking in the financial sector, and stands as a discussion point to provoke further work by academics and practitioners alike.

APPENDIX

The FDIC in its Electronic Banking document has identified six key areas of concern described as the unique risks associated with the electronic delivery of services:

1. Planning and Deployment: Key areas identified under this rubric include Impact of Technology on cost and pricing decisions; Systems design and capability not being able to met the customers demands; Implications of increasing competition from or involvement of non-financial entities; Uncertainty of blanket insurance coverage to or for electronic banking activities
2. Operating Policies and Procedures: Managerial or technical incompetence relative to electronic activities; controls inability to preserve confidentiality
3. Audit: Audit trails may be lacking
4. Legal and Regulatory: Enforceability of digital contracts, agreements, and signatures; User Privacy issues; Contingent liability resulting from user or participant claims; Legal jurisdiction with regards taxation, criminal and civil laws; Uncertain regulatory environment for electronic services (local or international); Applicability of reserve requirements to electronic money; Applicability of financial record keeping, disclosure and other requirements.
5. Administration and Systems Operation: Hardware and software failures or disruptions (Natural disasters, system attacks and participant failure); System or database compromise; Inadequate system capacity; System obsolescence; Administration of multiple standards and protocols; Systems security and control
6. Vendors and Outsourcing: Reliance on third party vendors for critical functions (Weak systems support and Internal controls issues); Maintenance and administration of multiple inter-related systems; Monitoring of inter-relationships among other participants in the payments system.

TABLE 1

Electronic Banking Statistics

YEAR	Number of cards outstanding	Total Commercial Banking Loans TT $'000	Credit Card Loans TT $'000	Credit Card Debt to Total Loans (%)
1993	49733	8123400	91998	1.13%
1994	63765	7158300	123499	1.73%
1995	75727	7662900	194809	2.54%
1996	89028	8146900	264918	3.25%
1997	109312	10010600	421380	4.21%
1998	126957	11454900	558191	4.87%
1999	134950	12325900	651236	5.28%

Source: Central Bank of Trinidad and Tobago

SELECTED REFERENCES

Anderton, Brian (eds.). *Current Issues in Financial Services.* 1995. Macmillan Press. London

Bank of England. 1992. *Financial Regulation: What are we trying to do?,* Quarterly Bulletin , 32(3)

European Central Bank. 1999. *The Effects of Technology on the EU Banking Systems,* July

Federal Deposit Insurance Corporation. 1999. "Information System Security Issues," July

Inter-American Development Bank. 2000. *Financial Risk Management: A practical approach for emerging markets*

Oldfield, George and Santomero, Anthony. 1997. *Risk Management in Financial Institutions.* Sloan Management Review Fall

Meyer, Lawrence. 2000. *Issues in Financial Modernization.*

Mitnick, B.M. 1980. The Political Economy of Regulation, New York, NY, Columbia University Press

Santomero, Anthony. 1997. Commercial Bank Risk Management: An analysis of the process. Wharton Financial Institutions Centre. University of Pennsylvania February

Spong, Kenneth 1994. *Banking Regulation: Its purposes, implementation, and effects.* 4th Edition. Federal Reserve Bank of Kansas City.

U.S. Comptroller of the Currency. 1999. *Internet Banking, Comptroller's Handbook,* October.

Wenninger, John. 1999. "Business to Business Electronic Commerce." *Current Issues in Economics and Finance 5, no 10 (June).*

Williams, Marion. 1996. *Liberalising a regulated Banking System: The Caribbean Case*