

E-BANKING AND EXTENDED RISKS: HOW TO DEAL WITH THE CHALLENGE?

Md. Atiqur Rahman Khan¹

Md. Masud Karim²

abstract

Continuous technological development, particularly, information technology revolution of the last two decades of the 20th century has forced the banks to introduce the e-banking operation for their sustainable growth in an expanded competitive environment. E-banking has made the financial transactions easier for the participants and has introduced wide range of financial products and services. At the same time it has amplified the existing risks as faced by traditional banks as well as has created new types of risks for banks. This paper presents a brief picture about all the risks associated with e-banking. It also highlights the ways of overcoming these risks.

Key words: E-banking, risks, security control.

1. INTRODUCTION

In the financial sector, last few decades have been under the sign of continuous liberalization and modernization. There is no doubt that technology is now the single biggest strategic issue in financial service. One of the most important revolutions created by the banking sector through using the new information and communication technologies, “under the guidance” of the Internet. Under the impact of the new technologies, new types of banking services have risen; the financial markets became more dilute and more efficient. A new but sound and effective concept 'electronic banking (e-banking)' has evolved.

The definition of e-banking varies amongst researchers partially because electronic banking refers to several types of services through which a bank customer can request information and carry out most retail banking services via computer, television or mobile phone (Daniel 1999; Molls 1998; Sathye 1999). Burr (1996) describes e-banking as an electronic connection between the bank and customer in order to prepare, manage and control financial transactions. On the other hand, Leow, Hock Bee (1999) state that the terms PC banking, online banking, Internet banking, telephone banking or mobile banking refers to a number of ways in which customer can access their banks without having to be physically present at the bank branch. The EBG of the Basel Committee on Banking Supervision³ (July 2003) noted that continuing technological innovation and competition among existing banking organizations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and

¹ Assistant Professor, Dept. of Finance & Banking, Rajshahi University.

² Assistant Professor, Dept. of Finance & Banking, Rajshahi University.

³ Electronic Banking Group of the Basel Committee on Banking Supervision, Bank for international settlements.

wholesale customers through an electronic distribution channel collectively referred to as e-banking.

Therefore, e-banking is a rather generic term and we need to be clear what we are talking about. E-banking can be separated into two streams: *electronic money products*, mainly in the form of stored value cards, and *electronic delivery channel products*. *Electronic money products* are issued in exchange for cash or deposit or credit. By debiting a deposit account or loan account of a financial institution and storing the value as data in an IC card beforehand, an individual can make payments for goods and services by transferring the electronic data stored in the card to the seller's card. It can also be termed as debit card. When such transactional opportunities are given on credit basis then it can be termed as credit card. On the other hand, *electronic delivery channel products* are arrangements for giving instructions for funds transfers, electronically. An individual can make payments for goods and services by giving instructions to debit its bank account and credit the seller's bank account through the exchange of electronic data through internet, mobile or television. These types products are also called the *access products*. E-banking, therefore, is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels.

E-banking can improve a bank's efficiency and competitiveness, so that existing and potential customers can benefit from a greater degree of convenience in effecting transactions. This increased level of convenience offered by the bank, when combined with new services, can expand the bank's target customers beyond those in traditional markets. Consequently, financial institutions are therefore becoming more aggressive in adopting electronic banking capabilities that include sophisticated marketing systems, remote-banking capabilities, and stored value programs. Internationally, familiar examples include telephone banking, automated teller networks, and automated clearinghouse systems. Such technological advances have brought greater sophistication to all users, commercial and "the man in the street".

Alongwith opportunities, e-banking generates extended risks for financial institutions. Degrees of existing risks that are associated with traditional banking have been widening as well as new types of risks have been evolved. E-banking increases banks' dependence on information technology, thereby increasing the technical complexity of many operational and security issues. This development has been leading to the creation of new business models involving banks and nonbank entities, such as Internet service providers, telecommunication companies and other technology firms. The Internet is ubiquitous and global by nature. It is an open network accessible from anywhere in the world by unknown parties, with routing of messages through unknown locations and via fast evolving wireless devices. Therefore, it significantly magnifies the importance of

security controls, customer authentication techniques, data protection, and customer privacy standards.

2. GLOBAL SCENARIO OF E-BANKING

The effect of e-banking is to augment or facilitate existing banking and payment mechanisms, primarily by making many transactions cheaper, faster, more secure, and more convenient. As a result such types of banking have been expanding day by day.

According to Forrester (November 2007), Online banking has grown gradually in the UK over the past decade and is now used by 31% of adults, or 15 million people. But growth has slowed in the past couple of years. That's odd because only 46% of UK Net users access their bank accounts online, yet 74% regularly shop online. By 2012, it is expected that 44% of adults to use online banking in the UK, or nearly 22 million people. Forrester (June 2009) projects that, between 2009 and 2014, the total number of US online bill payment households will increase from 48 million to 63 million.

Online banking has grown steadily in France over the past decade, boosted by the growth in Net use overall, and is now used by 31% of adults, or 15 million people. Growth to continue at a similar rate for the next five years because French Net users are becoming increasingly confident with the channel and because banks can still do more to persuade customers to bank online, starting with reducing or eliminating the charges that many still impose on customers who bank online. By 2013, it is expected that 42% of adults to use online banking, or more than 22 million people. (Forrester, February 2008).

With only 12% of Swedish banking customers using branches, Sweden has the lowest branch use in Europe. Swedish banks have successfully migrated the majority of their customers to ATMs and online banking — 83% and 71%, respectively. (Forrester May 2009).

Forrester also projects that, by 2012/20013, 81% of Dutch and 47% of German consumers will use Internet banking. (April 2008, November 2007).

In Bangladesh, there is huge demand for e-banking from the business community as well as the urban retail customers. But it is still not much available due to a number of constraints such as unavailability of a backbone network connecting the whole country; inadequacy of reliable and secure information infrastructure especially telecommunication infrastructure; sluggish ICT penetration in banking sector; insufficient legal and regulatory support for adopting e-banking and so on.

Although all branches of foreign commercial banks (FCBs) and 99 percent branches of private commercial banks (PCBs) in Bangladesh were computerized by December 2006, the average for all bank branches was 37 percent since only 4 percent and 16 percent of

specialized banks (SBs) and state-owned commercial banks (SCBs) respectively were computerized. Out of a total of 6,565 branches in 2006, 2,426 were computerized of which 651 branches of 22 PCBs and 7 FCBs together were providing any-branch-banking facility under respective bank online network. During the period, the number of ATM booths and POS terminals stood at 478 and 4,647 respectively covering important merchant outlets in six divisional cities and some other important district towns in Bangladesh while 43 banks became the member of SWIFT and 25 banks adopted router connection.⁴ Since about 50 percent of total bank branches belong to SCBs spread throughout the country including the rural areas, ICT penetration is crucial for this category of banks. The recent corporatization of the NCBs, would influence the banks in this category to be competitive through improving their service quality incorporating the use of modern technology. Although all these are positive developments, more attention is needed to enhance ICT capabilities of the banking system especially the SCBs for successful implementation of e-banking all over the country. (Rahman M. 2009).

3. RISKS RELATED WITH E-BANKING

Security vulnerabilities are part of web reality. The success of the internet has attracted a rising number of hackers and other scallywags. Thus, the internet, because of its low cost, global reach and versatility raises the stakes for the banks – both in terms of the opportunities it presents as well as the risks.

3.1 Strategic Risk

The cheapness and global reach of the internet opens up the threat of increased competition from new entrants who will no longer need a branch network to operate effectively in any given market. This competition can be launched across national frontiers. In the meantime, existing players are faced with the problem of what they do with the branch networks they have built up over the years.

Moreover, one of the key distinguishing characteristics of the internet is the ability which it gives customers to access and compare the offers of different banks. Internet also makes easier for the customer to get the banking services. This drives down banks' margins, particularly on commodity-type products, and erode customer loyalty. As has often been said, the Internet age is all about customer empowerment.

While the internet does indeed lower the barriers to entry, its anonymity and the vast range of choices also increase the importance of brand name. Depositors in particular will feel more comfortable with a name that they know and trust, and perhaps one whose name they see everyday in the street on signs above physical bricks and mortar. So banks with an existing brand name still have some advantage, but it is not something that can be wholly taken for granted. The banks will have to work hard to maintain and build

their brand image, and to offer products which differentiate themselves from their competitors.

A financial institution's board and management, therefore, should understand the strategic risk associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. Financial institutions should pay attention to the following:

- Adequacy of management information systems (MIS) to track e-banking usage and profitability;
- Costs involved in establishing e-banking technology;
- Design, delivery, and pricing of services adequate to generate sufficient customer demand;
- Costs and availability of staff to provide technical support for interchanges involving multiple operating systems, web browsers, and communication devices;
- Competition from other e-banking providers; and
- Adequacy of technical, operational, compliance, or marketing support for e-banking products and services.

3.2 Operational Risk

Operational or transaction risk is of course one of the more frequently mentioned risks in connection with electronic banking. Security concern is not new for banks. We are all familiar with the various security issues that banks are facing on a day-to-day basis, e.g. robberies, thefts of ATM machines, frauds. However, banking transactions over the internet do pose new issues.

Operational risk arises from fraud, processing errors, system disruptions, hacking, or other unanticipated events resulting in the institution's inability to deliver products or services. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

A major concern about the internet is its open nature. The key to controlling transaction risk lies in adapting effective policies, procedures, and controls to meet the new risk exposures introduced by e-banking. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level. Furthermore, continuing developments in security technology are required to maintain the effectiveness of security measures on an ongoing basis as new threats to existing

systems arise over time. Information security controls are discussed latter part of this paper.

3.3 Credit Risk

Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. However, management should consider additional precautions when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels. It is possible that credit risks could increase in the future if the relationship with customers becomes more distant and more transitory, and if the banks relax credit standards because of competitive pressures.

The following aspects of on-line loan origination and approval tend to make risk management of the lending process more challenging. If not properly managed, these aspects can significantly increase credit risk.

- Verifying the customer's identity for on-line credit applications and executing an enforceable contract;
- Monitoring and controlling the growth, pricing, and ongoing credit quality of loans originated through e-banking channels;
- Valuing collateral and perfecting liens over a potentially wider geographic area;
- Collecting loan payments from individuals over a potentially wider geographic area; and
- Monitoring any increased volume of, and possible concentration in, out-of-area lending.

3.4 Liquidity And Pricing Risks

Funding and investment-related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The ability to transfer funds between different bank accounts may increase deposit volatility and could, in extreme situations, lead to "virtual bank runs". Banks will need to consider this possibility into their liquidity management policies.

Internet-originated deposits have the potential to attract customers who focus exclusively on rates. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence. The institution should modify its policies as necessary to address the following e-banking funding issues:

- Potential acquisition of funds from markets where the institution is not licensed to engage in banking;
- Potential impact of loan or deposit growth from an expanded Internet market, including the impact of such growth on capital ratios; and
- Potential increase in volatility of funds due to the negative impact of customer confidence for e-banking security problems, or competitors' deposit or lending pricing policy.

3.5 Reputational Risk

An institution's decision to offer e-banking services, especially the more complex transactional services, significantly increases its level of reputation risk. Some of the ways in which e-banking can influence an institution's reputation include:

- Loss of trust due to unauthorized activity on customer accounts,
- Disclosure or theft of confidential customer information to unauthorized parties (e.g., hackers),
- Failure to provide reliable service due to the frequency or duration of service disruptions that is temporary systems breakdown;
- Customer complaints about the difficulty in using e-banking services and the inability of the institution's help desk to resolve problems, and

Risk of damage to the bank's reputation can also arise, even if customers suffer no actual damage. If a hacker successfully breaks into a bank's website and makes alterations, the bank concerned can suffer substantial damage to its reputation although customers' balances are safe and the hacker has not obtained any financial benefit. This does not only affect the individual bank concerned but may also undermine confidence in the security of e-banking more generally and therefore slow down development in this area.

3.6 Legal Risk

Legal risk becomes an important issue in internet banking, and one aspect of this is how any losses from security breaches should be apportioned between banks and their customers. Customers should be responsible for any security breach or system problem that is due to negligence on their part, and this should be reflected in the contractual agreements for internet banking services. But if the damage is occurred for system breakdown, negligence of bank employees, attack by hacker or any other parties; the bank must be liable to cover the damage.

4. RISKS MANAGEMENT

From the earlier discussions it is revealed that a bank may face different levels of risks arising from e-banking as opposed to traditional banking. Clearly, the longevity of e-banking depends on its accuracy, reliability and accountability.

The EBG of the Basel Committee on Banking Supervision (July 2003) expects such risks to be recognized, addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology.

The Committee has also identified fourteen "*risk management principles*" for electronic banking to help banking institutions. The *Risk Management Principles* fall into three broad, and often overlapping, categories of issues that are grouped to provide clarity: *Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management.*

A. Board and Management Oversight (Principles 1 to 3): The Board of Directors and senior management should-

1. establish effective management oversight over the risks associated with e-banking activities.
2. review and approve the key aspects of the bank's security control process.
3. establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

B. Security Controls (Principles 4 to 10): Banks should-

4. take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the Internet.
5. use transaction authentication methods that promote nonrepudiation and establish accountability for e-banking transactions.
6. ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
7. ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.
8. ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

9. ensure that clear audit trails exist for all e-banking transactions.
10. take appropriate measures to preserve the confidentiality of key e-banking information.

C. Legal and Reputational Risk Management (Principles 11 to 14): Banks should-

11. ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status.
12. take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.
13. effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.
14. develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

4.1 Information Security Control

Financial institutions have to consider these principles to minimize the risks discussed earlier. As such they need to develop a proper information security control system. Information security is essential to a financial institution's ability to deliver e-banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems. Financial institutions, therefore, must comply with the followings:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls.

- I. *Ongoing knowledge of attack sources, scenarios, and techniques.* Financial institutions should maintain an ongoing awareness of attack threats through membership in information-sharing entities such as the Financial Services -

Information Sharing and Analysis Center (FS-ISAC), Infragard, private mailing lists, and other security information sources.

- II. *Up-to-date equipment inventories and network maps.* Financial institutions should have inventories of machines and software sufficient to support timely security updating. In addition, institutions should understand and document the connectivity between various network components including remote users, internal databases, and gateway servers to third parties.
- III. *Network access controls over external connections.* Financial institutions have to carefully control external access through all channels including remote dial-up, virtual private network connections, gateway servers, or wireless access points. Typically, firewalls are used to enforce an institution's policy over traffic entering the institution's network. Firewalls are also used to create a logical buffer, called a "demilitarized zone," or DMZ, where servers are placed that receive external traffic. The DMZ is situated between the outside and the internal network and prevents direct access between the two.
- IV. *Controls to prevent malicious code.* Financial institutions should reduce the risks posed by malicious code by, among other things, educating employees in safe computing practices, installing anti-virus software on servers and desktops, maintaining up-to-date virus definition files, and configuring their systems to protect against the automatic execution of malicious code. Malicious code can deny or degrade the availability of computing services; steal, alter, or insert information; and destroy any potential evidence for criminal prosecution.
- V. *Rapid intrusion detection and response procedures.* Financial institutions should have mechanisms in place to reduce the risk of undetected system intrusions. Computing systems are never perfectly secure. When a security failure occurs and an attacker is "in" the institution's system, only rapid detection and reaction can minimize any damage that might occur. Techniques used to identify intrusions include intrusion detection systems (IDS) for the network and individual servers (i.e., host computer), and the identification and analysis of operational anomalies.
- VI. *Physical security of computing devices.* Financial institutions have to mitigate the risk posed by unauthorized physical access to computer equipment through such techniques as placing servers and network devices in areas that are available only to specifically authorized personnel and restricting administrative access to machines in those limited access areas. An attacker's physical access to computers and network devices can compromise all other security controls.

VII. *Authorized use policy.* Each financial institution should have a policy that addresses the systems various users can access, the activities they are authorized to perform, prohibitions against malicious activities and unsafe computing practices, and consequences for noncompliance. All internal system users should be trained in, and acknowledge that they will abide by, rules that govern their use of the institution's system.

4.2 Authenticating E-banking Customers

E-banking introduces the customer as a direct user of the institution's technology. Customers have to log on and use the institution's systems. Accordingly, the financial institution must control their access and educate them in their security responsibilities. While authentication controls play a significant role in the internal security of an organization, this section discusses authentication only as it relates to the e-banking customer.

4.2.1 Authenticating New Customers

Verifying a customer's identity, especially that of a new customer, is an integral part of all financial services. Each financial institution must develop and implement a customer identification program (CIP) that is appropriate given the institution's size, location and type of business. The CIP must be written, incorporated into the institution's Bank Secrecy Act/Anti-Money Laundering program, and approved by the institution's board of directors. The CIP must include risk-based procedures to verify the identity of customers (generally persons opening new accounts). Procedures in the program should describe how the bank will verify the identity of the customer using documents, nondocumentary methods, or a combination of both.

As part of its nondocumentary verification methods, a financial institution may rely on third parties to verify the identity of an applicant or assist in the verification. The financial institution is responsible for ensuring that the third party uses the appropriate level of verification procedures to confirm the customer's identity. New account applications submitted on-line increase the difficulty of verifying the application information. Many institutions choose to require the customer to come into an office or branch to complete the account opening process. Institutions conducting the entire account opening process through the mail or on-line should consider using third-party databases to provide:

- *Positive verification* to ensure that material information provided by an applicant matches information available from third-party sources,
- *Logical verification* to ensure that information provided is logically consistent, and
- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity (e.g., an address previously associated with a fraudulent application).

4.2.2 Authenticating Existing Customers

In addition to the initial verification of customer identities, the financial institution must also authenticate its customers' identities each time they attempt to access their confidential on-line information. Financial institutions should weigh the cost of the authentication method, including technology and procedures, against the level of protection it affords and the value or sensitivity of the transaction or data to both the institution and the customer.

Authentication methods involve confirming one or more of three factors:

- Something only the user should know, such as a password or PIN;
- Something the user possesses, such as an ATM card, smart card, or token; or
- Something the user is, such as a biometric characteristic like a fingerprint or iris pattern.

4.2.2.1 Password Administration

Some security professionals criticize passwords for a number of reasons. Password-cracking software and log-on scripts can frequently guess passwords regardless of the use of encryption.

Financial institutions that allow customers to use passwords with short character length, readily identifiable words or dates, or widely used customer information (e.g., National ID numbers/ Social Security numbers) may be exposed to excessive risks in light of the security threats from hackers and fraudulent insider abuse. Stronger security in password structure and implementation can help mitigate these risks. There are three aspects of passwords that contribute to the security they provide: password secrecy, password length and composition, and administrative controls.

- I. *Password secrecy.* The security provided by password-only systems depends on the secrecy of the password. If another party obtains the password, he or she can perform the same transactions as the intended user. Passwords can be compromised because of customer behavior or techniques that capture passwords as they travel over the Internet. Attackers can also use well-known weaknesses to gain access to a financial institution's (or its service provider's) Internet-connected systems and obtain password files. Because of these vulnerabilities, passwords and password files should be encrypted when stored or transmitted over open networks such as the Internet. The system should prohibit any user, including the system or security administrator, from printing or viewing unencrypted passwords. In addition, security administrators should ensure password files are protected and

closely monitored for compromise because if stolen an attacker may be able to decrypt an encrypted password file.

Financial institutions need to emphasize to customers the importance of protecting the password's confidentiality. Customers should be encouraged to log off unattended computers that have been used to access on-line banking systems especially if they used public access terminals such as in a library, institution lobby, or Internet cafe.

- II. *Password length and composition.* The appropriate password length and composition depends on the value or sensitivity of the data protected by the password and the ability of the user to maintain the password as a shared secret. Common identification items — for example, dictionary words, proper names, or social security numbers — should not be used as passwords. Password composition standards that require numbers or symbols in the sequence of a password, in conjunction with both upper and lower case alphabetic characters, provide a stronger defense against password-cracking programs. Selecting letters that do not create a common word but do create a *mnemonic* - for example the first letter of each word in a favorite phrase, poem, or song - can create a memorable password that is difficult to crack.

Attackers may use automated programs to systematically generate millions of alphanumeric combinations to learn a customer's password (i.e., "brute force" attack). A financial institution can reduce the risk of password compromise by communicating and enforcing prudent password selection, providing guidance to customers and employees, and careful protection of the password file.

- III. *Password administration controls.* When evaluating password-based e-banking systems, management should consider whether the authentication system's control capabilities are consistent with the financial institution's security policy. This includes evaluating such areas as password length and composition requirements, incorrect log-on lockout, password expiration, repeat password usage, and encryption requirements, as well as the types of activity monitoring. Each financial institution must evaluate the risks associated with its authentication methods given the nature of the transactions and information accessed.

4.2.2.2 Administrative Controls

E-banking activities are subject to the same risks as other banking processes. However, the processes used to monitor and control these risks may vary because of e-banking's heavy reliance on automated systems and the customer's direct access to the

institution's computer network. Some of the controls that help assure the integrity and availability of e-banking systems are discussed below.

- I. *Segregation of duties.* E-banking support relies on staff in the service provider's operations or staff in the institution's bookkeeping, customer service, network administration, or information security areas. However, no one employee should be able to process a transaction from start to finish. Institution management must identify and mitigate areas where conflicting duties create the opportunity for insiders to commit fraud.
- II. *Dual controls.* Some sensitive transactions necessitate making more than one employee approve the transaction before authorizing the transaction. Large electronic funds transfers or accesses to encryption keys are examples of two e-banking activities that would typically warrant dual controls.
- III. *Suspicious activity.* Financial institutions should establish fraud detection controls that could prompt additional review and reporting of suspicious activity. Some potential concerns to consider include false or erroneous application information, large check deposits on new e-banking accounts, unusual volume or size of funds transfers and multiple new accounts with similar account information or originating from the same Internet address.
- IV. *Similar website names.* Financial institutions should exercise care in selecting their website name(s) in order to reduce possible confusion with those of other Internet sites. Institutions should periodically scan the Internet to identify sites with similar names and investigate any that appear to be posing as the institution. Suspicious sites should be reported to appropriate criminal and regulatory authorities.
- V. *Error checks.* On-line forms can include error checks to identify common mistakes in various fields. Proactive confirmations can require customers to confirm their actions before the transaction is accepted for processing. For example, a bill payment customer would enter the amount and date of payment and specify the intended recipient. But, before accepting the customer's instructions for processing, the system might require the customer to review the instructions entered and then confirm the instruction's accuracy by clicking on a specific box or link.

5. CONCLUSION

Due to its lower transaction costs, twenty-four hours services, increased control over transactions, higher volume of transactions in less time, remote transaction facilities, and much wider array of banking products and services; e-banking has become an integral

part of modern banking. But besides these opportunities e-banking operation increases different levels of risks for banks. Furthermore, customers who rely on e-banking services may have greater intolerance for a system that is unreliable or one that does not provide accurate and current information. Through the advent of on-line services customer have greater choice and do not need to be tied to one financial institution or another. Clearly, the longevity of e-banking depends on its accuracy, reliability and accountability.

One of the major problem areas with Internet banking appears to be with the security and safeguarding of information exchanged between customer and bank. Indeed, the Federal Reserve Board of the US banking system expressed concern that the use of electronic banking could expose banks, their customers and their transactions to electronic interception and possibly interference leading to fraud. Therefore, banks need to conduct regular risk assessments, keep customers informed and, perhaps, be prepared to offer compensation if private information is made public. Therefore, all the risks associated with e-banking to be recognized, addressed and managed by banking institutions in a prudent manner. These risks can be mitigated by adopting a comprehensive risk management program that incorporates a sound strategic plan. Importantly, the extent of a financial institution's risk management program should be commensurate with the complexity and sophistication of the activities in which it engages.

E-banking requires new administrative controls and potentially increases the importance of existing controls. Management must evaluate its administrative controls to maximize the availability and integrity of e-banking systems. Effective incident response mechanisms are also critical to minimize operational, legal and reputational risks arising from unexpected events, including internal and external attacks that may affect the provision of e-banking systems and services.

REFERENCES:

Basel Committee On Banking Supervision, *Risk Management Principles for Electronic Banking*, Bank for international settlements. Access from: < <http://www.bis.org/publ/bcbs98.pdf>>

Burr, W. (1996), Wie Informationstechnik die bankorganisationverändernKonnte, *Bank und Markt* , Vol. 11, pp. 28-31.

Daniel, E. (1999), Provision of electronic banking in the UK and the Republic of Ireland, *International Journal of bank marketing*, Vol. 17, No. 2.

Deutsche Bank Research, *E-banking snapshot*, in Digital Economy, no 12, dec 2004, Access from:<www.dbresearch.com>

Forreester Research, *How Swedish Banking Customers Use Different Channels*, May 2009, access from: <www.forreester.com>

Forreester Research, *US Electronic Bill Payment And Presentment Forecast, 2009 To 2014*, June 2009, access from: <www.forreester.com>

Forreester Research, *French Online Banking Forecast: 2008 To 2013*, February, 2008, access from: <www.forreester.com>

Forreester Research, *Dutch Online Banking Forecast: 2008 To 2013*, April 2008, access from: <www.forreester.com>

Forreester Research, *German Online Banking Forecast: 2007 To 2012*, November 2007, access from: <www.forreester.com>

Forreester Research, *UK Online Banking Forecast: 2007 To 2012*, November 2007, access from: <www.forreester.com>

Leow, Hock, Bee. (1999), New Distribution Channels in Banking Services, *Bankers Journal Malaysia*, No. 110.

Mircea Georgescu (2006) *Some Issues about Risk Management for E-Banking*, accepted paper series Social Science Research Network.

Mols, K. (1998), The behaviour consequences of PC banking, *International Journal of bank marketing*, Vol. 16, No. 5, pp. 195-201.

Rahman, M. (2009), *E-banking in Bangladesh: Some Policy Implications*, Policy notes, Bangladesh Bank Quarterly, January-March 2009, Bangladesh Bank, Access from: <www.bangladeshbank.org.bd>

Rahman, M. (2008), *Innovative Technology and Bank Profitability: The Bangladesh Experience*, Working paper series 0803, Research Work, Policy Analysis Unit (PAU), Bangladesh Bank, Access from:<www.bangladeshbank.org.bd>

Sathye, M. (1999), Adoption of Internet banking by Australian customers, *International Journal of bank marketing*, Vol. 17, No. 7, pp. 324-334.