Research Journal of Information Technology 5(2): 50-54, 2013
ISSN: 2041-3106; e-ISSN: 2041-3114

Submitted: December 23, 2012 Accepted: February 01, 2013 Published: June 01, 2013

Online Banking and the Risks Involved

Olufolabi Osunmuyiwa
No 11 Guzerin St., Cyprus

Abstract: This study aims to expand on the various aspects of online banking risks and the risk management methods employed in mitigating these risks. Ongoing hi-tech improvement and rivalry between available banking organizations and latest participants have permitted for a much extensive range of banking products and services to grow to be available and distributed to retail and wholesale clients via an electronic allocation channel jointly referred to as online banking. Nevertheless, the swift improvement of online banking potentials holds threats as well as opportunities and strengths. This study will expand more on various aspects of online banking risks such as strategic risk, transaction risk, compliance risk, reputation risk, information security risk, credit risk, interest rate risk, liquidity risk, price risk and foreign exchange risk, with the risk management methods. These risks should be acknowledged, attended to and controlled by banking establishments in a cautious approach according to the elementary attributes and challenges of online banking services. These attributes consist of the unique pace of change associated to hi-tech and client service improvement, the ever-present and global character of open electronic networks, the incorporation of online banking applications with heritage computer systems and the greater than ever reliance of banks on third parties that make available the required information technology. While not creating innately most modern risks, these attributes amplified and modified some of the traditional risks connected with banking activities, particularly strategic, operational, legal and reputational risks, in so doing influencing the general risk outline of banking. Due to these conclusions, accessible risk management principles stay appropriate for online banking activities and such principles ought to be personalized, adapted and, in some cases, expanded to deal with the precise risk management challenges fashioned by the attributes of online banking activities. These "Risk Management Principles" are not present as total prerequisites. Implementing comprehensive risk management prerequisites in the region of online banking may be counter-productive, if only for the reason that these would be likely to grow to be swiftly outmoded because of the pace of change associated to hi-tech and client service upgrading. Nevertheless, some concerns, such as the organization of outsourcing relationships, security controls and legal and reputational risk management, necessitate more comprehensive values than those articulated to date owing to the distinctive attributes and repercussions of the internet allotment channel.

Keywords: Online banking and risk

INTRODUCTION

Internet banking of marketplace: Presently, the marketplace makes use of three fundamental types of internet banking (Internet Banking Comptroller's Handbook, 1999):

- **Informational:** Referred to as a fundamental stage of online financial transaction. It provides information concerning the bank's products and services. A separate server is usually available to any financial institution to contain transaction data of services and goods. The peril is comparatively reduced, due to the absence of a course in data systems linking the financial institution's system and the server. Although threats aimed at financial institutions are comparatively small, high susceptibility to fluctuations could occur to the network or webpage. Proper methods of regulation consequently should be laid down to avert illicit fluctuations to the financial organization's network and webpage (Gunajit and Pranav, 2010).
- **Communicative:** This form of online financial transactional method permits communication between a financial organization and the client. It provides account-related data and updates to fixed information like addresses. The communication could get restricted to electronic correspondence, financial credit inquisition, or credit requests. Fitting management should be laid down avert, supervise and prepared high ranking members of whichever illegal effort to gain entry into the financial institution's interior systems. Use of antivirus is very important in this atmosphere (Gunajit and Pranav, 2010).
- **Transactional:** This height of internet banking permits clients to carry out transactions. It permits clients to carry out financial transactions even if

the client has never physically been to bank. Since a trail naturally exists amid the server and the bank's or outsourcer's interior network, this is the greatest threat frame work and should posses a tough regulator. Client business deal could involve the transfer of money, checking of account balance and so on Gunajit and Pranav (2010).

Nowadays banks visualize economic returns by applying electronic banking processes for clients connected to the internet through personal computers, mobile phones and tablets thus increasing the risk of an online banking transaction.

Features of online banking:

Transactional: It involves carrying out financial transactions such as payment of bills, applying for a loan and enrollment repayments, creating a new account, invest purchase and sales and transfer of funds between a clients' transactional account and a savings account (Boni and Tsekeris, 2007).

Non transactional: It involves downloading of financial documents like a bank statement, co browsing, checking of links and viewing of recent financial transactions such as viewing images of paid cheques (Gandy, 1995).

Transaction approval process: The Transaction Approval Process (TAP) permits an institute to make use of Access Online to endorse and review transactions through existing interior approval hierarchy and methods. The TAP utility is used to get rid of paper endorsements and effortlessly approve transactions and view endorsement record. The TAP function's elasticity also permits the client mirror his or her own interior reviewing methods, from simple to complex (Access Online Transaction Approval Process User Guide, 2009).

TAP function is utilized by two fundamental users (John, 2012):

- Cardholders, who utilizes' TAP to approve and further transactions to an endorsement director.
- Endorsement director, who utilizes' TAP to evaluate, approve lastly and further (provided it is required) transactions to another endorsement director.

The arrangement allows merely a single user to amend a transaction at a known period of time. This attribute decreases the likelihood of scam and guarantees that just a single user can amend a transaction at a time. Mutually cardholders and endorsement directors can carry out these subsequent fundamental practices:

- **Approve transactions:** Cardholders and endorsement directors can approve transactions and further them to an endorsement director for added endorsement. Cardholders approve and further personal transactions, while endorsement directors approve and further transactions from cardholders and other endorsement directors.
- **Retract transactions:** Cardholders and endorsement directors can retract transactions that an endorsement director has not approved, discarded, or personalized.
- **Supervise discarded transactions:** Endorsement directors and cardholders can handle transactions that endorsement directors decline.

Mobile banking: It gives clients the ability to carry out financial operations at anytime of the day, at anywhere. This is aided by the use of mobile device companies such as Apple and Research in Motion (RIM), that produce mobile phones and electronic tablets that make online banking easier (Vaidya, 2011).

MATERIALS AND METHODS (ONLINE BANKING RISKS)

The internet and technological advancements with the beginning of vend and commercial financial transactional options have differentiated the precedent years. The degree of peril financial institutions are opened has been intensified due to factors such as an ever present and universal character of electronic systems, exceptional pace through which innovative equipments are recognized, incorporation of online financial transaction policies and heritage networks with the growing reliance of financial institutions on outsourcing (Natasha, 2012).

Numerous financial institutions understand that online transaction principally enhance data protection perils with little or no attention being paid towards the consequence involving further financial transaction-precise perils. Controls involving the supervision of perils are developing at a slow pace when compared to the momentum at which loads of organizations are growing without the integration of risk management principles in their business arrangements (Ganesh, 2001). This chapter presents a general idea of a variety of risks keen to online financial transaction, with well defined methods of controlling these perils.

Categories of online banking risks: Online financial transactions do not create fresh peril groups, but to a certain extent draws attention to the risks that several monetary establishment faces (Michael and Herbert, 2009). The board and higher ranking executive must be mindful of these risks and see to them suitably. These risks, which have common characteristics, for a moment, are explained next:

- **Transactional risk:** Described as the recent and potential peril to income and investment coming up from hoax, blunder, disregard and the incapability to sustain anticipated service intensity. An elevated intensity of business risk may exist with online banking products, due to the necessity to have refined interior controls and regular accessibility. A good number of platforms in financial transactions are footed on innovative backgrounds that connect with heritage networks using intricate interfaces, in so doing increasing the blunders likely to occur while carrying out a transaction. The need for non refutation of transaction and the ability to guarantee data should not be overlooked. The presence of third-party suppliers add to perils associated with financial transactions, giving that no total power over the third-party is possessed by the institution. There is an elevated risk of transaction errors even in the presence of system links and absence of faultless procedures between the bank and the third party [*http:// internetbanking.tv/internet-banking-risks/*].
- **Compliance risk:** Described as the recent and potential peril to income or investment arising due to the inability to conform to, or infringements of, decrees, guidelines and moral values. Perils associated with being compliant might bring about lessened status, tangible financial fatalities and reduced business opportunities. Banks should cautiously comprehend and read between the lines presented laws seeing that they pertain to online banking and guarantee regularity with other controls like branch banking. The peril is significantly increased when the financial transaction, customer or the bank is located in more than one country and also by contradictory regulations, tax practices and treatment obligations athwart diverse jurisdictions. The necessity to maintain client information confidential and inquire about clients' permission prior to giving out the information further more increases the risk of being compliant. Banks should be regarded as reliable custodians of financial data because when it comes to data confidentiality, customers are highly apprehensive (Gunajit and Pranav, 2010).
- **Reputation risk:** Described as the risk to income and investment caused by unenthusiastic public view. A financial institution's status could get dented through online financial transactions carried out defectively (such as restricted accessibility, or reduced reaction). Additional severe performance prospects are expected from online channels due to lack of patient from customers who care less of whichever predicament the financial institution has found itself (Ganesh, 2001).
- **Risks associated with information security:** Described as the risk to income and investment arising due to negligent data safekeeping procedures, consequently revealing the organization to scam, information obliteration, virus, information thieves, vicious hacker, insider assaults and Denial-of-Service (DoS) attacks. The peril is serious due to the fast pace seen in the transformation of technology, with the reality that the online channel is easily reached (Ingo, 2007) (Fig. 1).

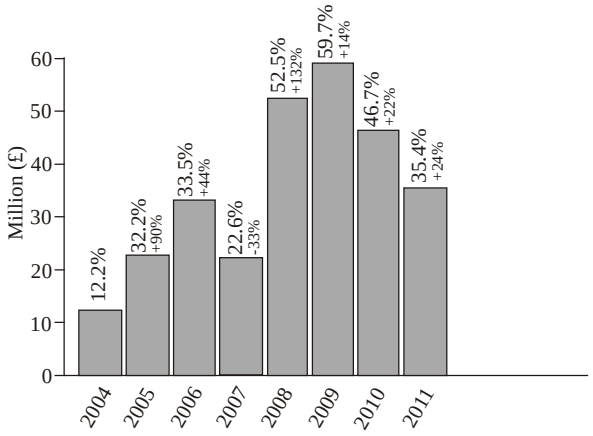

Fig. 1: Online banking fraud losses 2004-2011, http://www.google.com/imgres?q=percentage+of+online+banking+risks+2012

RESULTS AND DISCUSSION (RISK MANAGEMENT PRINCIPLES)

The risk should be assessed based on the category of client, the organization's transactional abilities, the importance and worth of the amassed data to the organization and client, the simplicity of using the scheme and with degree and magnitude of transactions. Running the risks and putting into practice controls for online banking schemes tags along very similar standards with likewise procedures of managing risks (James, 2005). Leaving this to "Information Technology (IT)" to manage or indulging it as a technical setback can be a very unsafe thing to do. As above listing of risks have suggested, there is a need for a top managerial role in order to effectively monitor and combat these risks.

Board and management oversight: The top managerial staff of the banking institution is obliged to ensure the effective management of all forms of risks associated with online banking and also ensure accountability and policy control in the execution of activities related to E-banking. Also the top managerial officers should maximize to the fullest the opportunities attached to online banking such as garnering of profits and to fulfill the main goals and objectives of the institution. An unmistakable intention sets the tone for a healthy risk position.

It is the responsibility of high ranking officers to evaluate and endorse the transactional report of the online banking as lack of evaluation could result into a big problem for the institution. The report should be tactically analyzed and should be subjected to affordable cost auditing. Also, top managerial officers should not be involved in e-banking enterprise unless they are highly horned in risk management.

Also the top managerial staff of any banking institution should decide the method of risk management, reporting approaches and intensification methods. An official risk analyses group should be appointed by the top managerial staff in line with accountability, risk evaluation, alleviation and recognition. Also top managerial staff should ensure thorough analyses of online banking before it is embarked upon [*http://www.bis.org/publ/bcbs82.htm*].

Legal and reputational risk management: Legal and reputational risk management can be divided into the following:

- **Privacy:** There should be a privacy rule from the bank and this must be communicated to all prospective clients. Clients have to be given the opportunity to withdraw whenever required and this should be laced with different alternatives of choice. Also client permission should be sought before dissemination of information to external parties. Finally if clients are from different locales, the strongest privacy law is therefore applicable [*http://ithandbook.ffiec.gov/it-booklets/ e-banking/ risk-management -of-e-banking-activities/ board-and-management- oversight. aspx.*].
- **Availability:** Business stability and emergency planning strategy which guarantees ease of accessibility of online banking services to customers must be included by the banking institution. This however is highly demanding based on the 24 h provision of services and accessibility to customers and also the amount of transactions carried out (Weber Shandwick, 2012).
- **Incident response:** There should be the creation of s device which identifies, contain and handles promptly difficulties that might arise both internally and externally. There should be a communication blueprint for clients by whom they can channel their complaints and the use of intensification pathways. Finally a medium by which forensic evidence is protected in the case an assault should be created (Ganesh, 2001).

Excel Spreadsheet for Risk Assessment for Policies, Training for Risk Assessment, Cover Sheet, Vendor Oversight, Assignment Sheet, amongst others are instruments created from a range of data resources to carry out risk evaluation on data safekeeping and/or Online banking. The worksheets cuts across instructing matters, agreement issues, board and management supervision and risk evaluations for guarding principles from a variety of disaster recuperation to wire transfers.

The risks that crops up from online banking are not limited to protection of information but can be seen to have its own effects on other areas of the banking system. There is a need for the integration of risk management by top managerial staff and this should be done in accordance with already existing regulatory mechanisms in the organization. In cases of technological modifications, control processes are expected to be upgraded. When it comes to human resource risk management in online banking, cautious methods should be practiced to prevent existing and past members of staff, service providers, vendors and those who possess a key understanding of the internal workings of the bank's systems, operations and inner controls that have a major advantage over external attackers from carrying out attacks on the bank's clients (Weber Shandwick, 2012).

Simple guidelines for safe online banking:

- On no account utilize communal terminals like cyber cafes when you are carrying out banking transactions online.
- The peril of compromise while making use of a wireless connection is to a large extent greater. Clients should carry out online banking transactions through a wireless connection provided that they are completely assured of the connection safety.
- Clients should be certain that their spyware and anti-virus applications are up to date and it is advisable to perform regular system scans.
- Clients should on no account log into a banking site via a link. Alternatively, clients should type out the address of the bank's website into the browser bar.
- Clients should never access any other web site when they are logged into an online banking site; they should be sure as to ascertain that there is only one window open.
- Clients should choose their user name and password cautiously. Both password and user name shouldn't be easy for anyone to deduce and they should be changed regularly.
- Client's computer software should be updated regularly.
- Clients should check for the padlock logo on the lesser right hand side of the browser window (it shows that the website is secured).
- Once a client is done with his or her Online banking, the client should log out and close the browser window.

- On no account should a client give out his or her password on the Internet (via emails) or through the phone to anybody.

CONCLUSION

Online banking is a structure that enables people executes banking actions via the internet at their homes and other private places at any selected time without the need to physically be in a bank.

Online banking risks should be acknowledged attended to and controlled by banking establishments in a cautious approach based on the rudimentary attributes and problems of online banking services. Accessible risk management principles stay appropriate for online banking activities and such value propositions ought to be personalized, modified and, perhaps extended to deal with the precise risk management dilemmas fashioned by the attributes of online banking activities. Online banking does not create novel risk groups, but to a certain extent draws attention to the risks that several monetary establishment faces and risk management controls have not developed at very similar momentum and loads of institutions, particularly the less important ones, have been incapacitated in their drive to integrate online banking risk management inside their present risk management arrangements. The risks should be based on the category of client, the organization's transactional abilities, the importance and worth of the amassed data to the organization and client, the simplicity of using the scheme and with degree and magnitude of transactions.

It is widely recommended that banks that carry out online banking clearly explain the privacy rule and communicate it to their clients. Banks can also make use of materials like Vendor Oversight, Assignment Sheet and Excel Spreadsheet for Risk Assessment for Policies amongst so many created from a range of data resources to carry out data safekeeping.

ACKNOWLEDGMENT

We are grateful to the department of Information Technology, Eastern Mediterranean University and to Folahan Osunmuyiwa for her support and encouragement.

REFERENCES

Access Online Transaction Approval Process User Guide, 2009. Retrieved from: http://www. vanderbilt.edu/procurement/pcard/forms/Transaction%20Approval%20Guide.pdf.

Boni, K. and C. Tsekeris, 2007. Electronic Banking. In: Ritzer, G. (Ed.), Blackwell Encyclopedia of Sociology, Blackwell Reference Online. Retrieved from: en.wikipedia.org/wiki/Online_banking.

Gandy, T., 1995. Banking in e-space. Banker, 145(838): 74-76.

Ganesh, R., 2001. Risk management for internet banking. Inform. Syst. Cont. J., 6: 48-50.

Gunajit, S. and K.S. Pranav, 2010. Internet banking: Risk analysis and applicability of biometric technology for authentication. Int. J. Pure Appl. Sci. Technol., 1(2): 67-78.

Ingo, W., 2007. Reputational Risk and Conflicts of Interest in Banking and Finance: The Evidence So Far. APIF, Social Science Research Network, December 20, Retrieved from: http://papers. ssrn.com/ sol3/papers. cfm?abstract_id=952682.

Internet Banking Comptroller's Handbook, 1999. Comptroller of the Currency Administrator of National Banks. October 1999, USA.

James, A.N., 2005. Information security risk in financial institutions. World Acad. Sci. Eng. Technol., 10: 58-60.

John, T., 2012. Retrieved from: http://www. targusinfo. com/files/PDF/white_papers/OnlineTransactionApprovalBestPractices.pdf.

Michael, E.W. and J.M. Herbert, 2009. Priciples and Practices of Information Security. Cenage Learning, Indian Edition.

Natasha, B., 2012. Retrieved from: http://www. buzzle. com/articles/advantages - and - disadvantages - of - online-banking-services.html.

Vaidya, S.R., 2011. Emerging trends on functional utilization of mobile banking in developed markets in next 3-4 Years. Int. Rev. Bus. Res. Papers, 7(1): 301-312.

Weber Shandwick, 2012. Managing Legal and Reputational Risk: A View from the Field, Retrieved from: http://www. webershandwick. com/resources.