**Journal of Advanced Computing and Communication Technologies** ***(ISSN:* 2347 - 2804*)***
***Volume No.5 Issue No.3, June 2017***

# E-BANKING – INFLUENCE, THREATS and SECURITY

By
Dr. Neha Paliwal

1st Asst. Prof. Mahaveer College of Commerce.

1stpaliwals.neha@gmail.com

## ABSTRACT
The advancement of electronic banking (e-banking) began with the utilization of automatic teller machines (ATMs)and has incorporated telephone banking, direct bill payment, electronic fund transfer and online banking.According to some, the future direction of e-banking is the upliftment of mobile and telephone (WAP-enabled)banking and interactive-TV banking. In any case, it has been forecast by many that online banking willcontinue to be the most popular method for future electronic financial transactions.Electronic funds transfer (EFT), alludes to the usage of computer-based systems for perform financialtransaction electronically. The term is used for a number of diverseideas including electronicpayments and cardholder-initiated transactions, where a cardholder makes utilization of a payment card such asa credit card or debit card. Card-based EFT transactions are often covered by the ISO 8583 series ofstandards.

## Keywords
e-banking, e-commerce, e-banks.

## 1.Introduction
In order for clients to utilize their banks e-banking services they need to have a personal computer andinternet connection. Their personal computer becomes their virtual banker who will assist them in their banking errands. Examples of e-banking services that clients can get online are:
• Attaining information about accounts and loans,
• Conducting transfers amongst diverse accounts, even between external banks,
• Paying bills,
• Buying and selling stocks and bonds by depot,
• Buying and selling fund shares39
These services that are offered by e-banking are changing and being enhanced because of the intensecompetition between the banks online. Banking industry must adapt to the electronics age, which in its turnis changing all the time.
EFT transactions require authorization and a method to authenticate the card and the card holder. Whereasa merchant may physically verify the card holder's signature, EFT transactions require the card holder's PINto be sent online in an encrypted form for validation by the card issuer. Other information may be incorporatedin the transaction, some of which is not visible to the card holder (for instance magnetic stripe data), andsome of which may be requested from the card holder (for instance the card holder's address or the CVV2security value printed on the card).
EFT transactions are activated during e-banking procedures. Various methods of e-banking include:
• Telephone banking
• Online banking
• Short Message Service (SMS) banking
• Mobile banking
• Interactive-TV banking .

## 2.Influence of e-banking on conventional banking services
One of the issues right now being addressed is the influence of e-banking on conventional banking players. Afterall, if there are threats inherent in going into e-banking there are other threats in not doing so. It is too early tohave a firm opinion on this yet. Even to practitioners the future of e-banking and its implications are unclear.It might be convenient nevertheless to outline briefly two opinions that are prevalent in the market.
The opinion that the internet is a revolution that will sweep away the old order holds much away. Argumentsin favour are as follows:
• E-banking transactions are much cheaper than branch or even phone transactions. This could turnprevious competitive advantage - a vast branch network, into a comparative disadvantage,allowing e-banks to undercut bricks-and-mortar banks. This is commonly known as the "beacheddinosaur" theory.
• E-banks are easy to set up so lots of new participants will arrive. 'Old-world' systems, cultures andstructures will not encumber these new participants. Instead, they will be adaptable and responsive. E-bankinggives consumers much more choice. Consumers will be less inclined to remain loyal.
• E-banking will lead to an erosion of the 'endowment effect' right now enjoyed by the most of the banks.
Deposits will go elsewhere with the consequence that these banks will have to fight to regain andretain their utilization base. This will increase their cost of funds, possibly making their business lessviable. Lost revenue may even result in these banks taking more threats to breach the gap.
Portal providers are probably to attract the most significant share of banking profits. Indeed banks couldbecome glorified marriage brokers. They would simply bring two parties together – eg buyer and seller,payer and payee.
The products will be provided by monolines, experts in their field. Conventional banks may simply be leftwith payment and settlement business – even this could be cast into doubt.Conventional banks will find it difficult to evolve. Not

only will they be unable to make acquisitions for cashas opposed to being able to offer shares, they will be unable to obtain additional capital from the stockmarket. This is in opposite to the situation for internet firms for whom it seems relatively easy to attractinvestment.

There is of course another opinion which sees e-banking more as advancement than a revolution.

E-banking is just banking offered via a new delivery channel. It simply gives consumers another service(just as ATMs did).Like ATMs, e-banking will influence on the nature of branches but will not remove their value.Conventional banks are starting to fight back.The start-up expenses of an e-bank are high. Setting up a trusted brand is very costly as it requires significantadvertising expenditure in addition to the purchase of expensive technology (as security and privacy arekey to gaining user approval).E-banks have already found that retail banking only becomes profitable once a vast critical mass isachieved. Consequently many e-banks are limiting themselves to providing a tailored service to the betteroff.

Nobody truly knows which of these versions will triumph. This is something that the market willdetermine. In any case, supervisors will need to pay close attention to the Influence of e-banks on the conventionalbanks, for example by surveillance of:

- strategy
- utilization levels
- earnings and expenses
- advertising spending
- margins
- funding expenses
- merger opportunities and threats.

## 3.Threats

Banking on the Internet provides benefits to the consumer in terms of convenience, and to the provider in terms of cost reduction and greater reach. The Internet itself however is not a secure medium, and thus poses a number of risks of concern to regulators and supervisors of banks and financial institutions. As figure 1 shows the threats associated with e- banking.


Fig :1- Threats associated with e-banking

**Strategic threat**- A financial institution's board and management should understand the threats associatedwith e-banking services and evaluate the resulting threat management expenses against the potential return oninvestment prior to offering e-banking services. Poor e-banking planning and investment decisions canincrease a financial institution's strategic threat. On strategic threat e-banking is relatively new and, as a result,there can be a lack of understanding among senior management about its potential and implications. Peoplewith technological, but not banking, skills can end up driving the initiatives. E-initiatives can spring up inan incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost.Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract thetypes of utilizations that banks want or expect and may have unexpected implications on existing businesslines.Banks should respond to these threats by having a clear strategy driven from the top and should ensure thatthis strategy takes account of the effects of e-banking, wherever relevant. Such a strategy should be clearlydisseminated across the business, and supported by a clear business plan with an effective means ofmonitoring performance against it.

**Business Threats**- Business Threats are also significant. Given the newness of e-banking, nobody knows muchabout whether e-banking utilizations will have diverse characteristics from the conventional bankingutilizations. They may well have diverse characteristics. This could render existing score card models inappropriate, this resulting in either higher rejection rates or inappropriate pricing to cover the threat. Banksmay not be able to assess credit quality at a distance as effectively as they do in face to face circumstances.It could be more difficult to assess the nature and quality of collateral offered at a distance, especially if it is located in an area the bank is unfamiliar with (particularly if this is overseas). Furthermore as it isdifficult to predict utilization volumes and the stickiness of e-deposits (things which could lead either torapid flows in or out of the bank) it could be very difficult to manage liquidity.

Of course, these are old threats with which banks and supervisors have considerable experience but they needto be watchful of old threats in new guises. In particular threat models and even processes designed forconventional banking may not be appropriate.

**Legal and ethical Threats-** Legal risk arises from violation of, or nonconformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. Given the relatively new nature of Internet banking, rights and obligations in some cases are uncertain and applicability of laws and rules is uncertain or ambiguous, thus causing legal risk. Other reasons for legal risks are uncertainty about the validity of some agreements formed via electronic media and law regarding customer disclosures and privacy protection. A customer inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions. In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer. If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risks. A digital certificate is intended to ensure that a given signature is, in fact, generated by a given signer . Because of this, the certifying bank may become liable for the financial losses incurred by the party relying on the digital certificate.

**Transaction/operations threats** - Transaction/Operations threat arises from fraud, processing errors, systemdisruptions, or other unanticipated events resulting in the institution's inability to deliver products orservices. This threat exists in each product and service offered. The level of transaction threat is affected by thestructure of the institution's processing environment, including the types of services offered and thecomplexity of the processes and supporting technology.

In most instances, e-banking activities will increase the complexity of the institution's activities and thequantity of its transaction/operations threat, especially if the institution is offering innovative services thathave not been standardized. Since users expect e-banking services to be available 24 hours a day, 7days a week, financial institutions should ensure their e-banking infrastructures contain sufficient capacityand redundancy to ensure reliable service availability. Even institutions that do not consider e-banking acritical financial service due to the availability of alternate processing channels, should carefully considerclient expectations and the potential Influence of service disruptions on client satisfaction and loyalty.

The key to controlling transaction threat lies in adapting effective polices,procedures, and controls to meetthe new threat exposures introduced by e-banking. Basic internal controls including segregation of duties,dual controls, and reconcilements remain important. Information security controls, in particular, becomemore significant requiring additional processes, tools, expertise, and testing. Institutions should determinethe appropriate level of security controls based on their assessment of the sensitivity of the information tothe users and to the institution and on the institution's established threat tolerance level.

**Money Laundering Threats** -As Internet banking transactions are conducted remotely, banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal Recent Researches in Artificial Intelligence, Knowledge Engineering and Data Bases ISBN: 978-960-474-273-8 136 sanctions for non-compliance with "know your customer" laws. To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

**Cross border threats -** Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks. It includes legal and regulatory risks, as there may be uncertainty about legal requirements in some countries and jurisdiction ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risks associated with noncompliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws. If a bank uses a service provider located in another country, it will be more difficult to monitor it thus, causing operational risk. Also, the foreign-based service provider or foreign participants in Internet banking are sources of country risk to the extent that foreign parties become unable to fulfill their obligations due to economic, social or political factors. Cross border transaction accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base.

**Reputational Threats**- This is considerably heightened for banks using the internet. For example the internetallows for the rapid dissemination of information which means that any incident, either good or bad, iscommon knowledge within a short space of time. The speed of the internet considerably cuts the optimalresponse times for both banks and regulators to any incident.Any problems encountered by one firm in this new environment may affect the business of another, as itmay affect confidence in the Internet as a whole. There is therefore a threat that one rogue e-bank couldcause significant problems for all banks providing services via the internet. This is a new type of systemicthreat and is causing concern to e-banking providers. Overall, the Internet puts an emphasis on reputationalThreats. Banks need to be sure that users rights and information needs are adequately safeguarded andprovided for.

**Traditional Threats** -Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in Internet banking. These risks get intensified due to the very nature of Internet banking on account of use Recent Researches in Artificial Intelligence, Knowledge Engineering and Data Bases ISBN: 978-960-474-273-8 137 of electronic channels as well as absence of geographical limits . However, their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in Internet banking.


Fig:2- Threats/risks associated with traditional banking.

**Credit threat** - Generally, a financial institution's credit threat is not increased by the mere fact that a loan isoriginated through an e-banking channel. In any case, management should consider additional precautionswhen originating and approving loans electronically, including assuring management information systemseffectively track the performance of portfolios originated through e-banking channels. The followingaspects of on-line loan origination and approval tend to make threat management of the lending process morechallenging. If not properly managed, these aspects can significantly increase credit threat.

• Verifying the customer's identity for on-line credit applications and executing an enforceable contract;
• Monitoring and controlling the growth, pricing, underwriting standards and ongoing credit quality ofloans originated through e-banking channels;
• Monitoring and oversight of third-parties doing business as agents or on behalf of the financialinstitution (for example, an Internet loan origination site or electronic payments processor);
• Valuing collateral and perfecting liens over a potentially wider geographic area;
• Collecting loans from individuals over a potentially wider geographic area;
• Monitoring any increased volume of, and possible concentration in, out-of-area lending.

**Liquidity, interest rate, price/market Threats -** Funding and investment-related threats could increase with aninstitution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. TheInternet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits.But internet-originated deposits have the potential to attract utilizations who focus exclusively on rates andmay provide a funding source with threat characteristics similar to brokered deposits. An institution cancontrol this potential volatility and expanded geographic reach through its deposit contract and accountopening 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 increase in dependence on brokered funds or other highly rate-sensitive deposits;
• Potential acquisition of funds from markets where the institution is not licensed to engage in banking,particularly if the institution does not establish, disclose, and enforce geographic restrictions;
• Potential influence of loan or deposit growth from an expanded internet market, including the Influence ofsuch growth on capital ratios;
• Potential increase in volatility of funds should e-banking security problems negatively influenceclients confidence or the market's perception of the institution.

**Security Threats**

Security is one of the most discussed issues around e-banking.E-banking increases security threats, potentially exposing hitherto isolated systems to open and risky environments.Security breaches essentially fall into three categories; breaches with serious criminal intent (fraud, theft ofcommercially sensitive or financial information), breaches by 'casual hackers' (defacement of web sites or'denial of service' - causing web sites to crash), and flaws in systems design and/or set up leading tosecurity breaches (genuine users seeing / being able to transact on other users accounts). All of thesethreats have potentially serious financial, legal and reputational implications.Many banks are finding that their systems are being probed for weaknesses hundreds of times a day butdamage/losses arising from security breaches have so far tended to be minor. In any case some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency ofunsuccessful attempts to break into their system.The most sensitive computer systems, such as those used for high value payments or those storing highlyconfidential information, tend to be the most comprehensively secured. One could therefore imply that thegreater the potential loss to a bank the less probably it is to occur, and in general this is the case. In any case,while banks tend to have reasonable perimeter security, there is sometimes insufficient segregationbetween internal systems and poor internal security. It may be that someone could breach the lightersecurity around a low value system.It is easy to overemphasize the security threats in e-banking. It must be remembered that the internet couldremove some errors introduced by manual processing (by increasing the degree of straight throughprocessing from the user through banks' systems). This reduces threats to the integrity of transactiondata (although the threat of users incorrectly inputting data remains). As e-banking advances, focusinggeneral attention on security threats, there could be vast security gains.Financial institutions need as a minimum to have:
- A strategic approach to information security, building best practice security controls into systemsand networks as they are developed
- A proactive approach to information security, involving active testing of system security controls (e.g. penetration testing), rapid response to new threats and vulnerabilities and regular review ofmarket place developments
- Sufficient staff with information security expertise
- Activeutilization of system based security management and monitoring tools
- Strong business information security controls.

These are the issues line supervisors will be raising with their banks as part of their on-going supervision.

## 4.Conclusion

In conclusion e-banking creates issues for banks and regulators alike. For their part, banks should:
• Have a clear and widely disseminated strategy that is driven from the top and takes intoaccount the effects of e-banking, together with an effective process for measuringperformance against it.
• Take into account the effect that e-provision will have upon their business threat exposures andmanage these accordingly.
• Undertake market research, adopt systems with adequate capacity and scalability, undertakeproportional advertising campaigns and ensure that they have adequate staff coverage and asuitable business continuity plan.
• Ensure they have adequate management information in a clear and comprehensible format.
• Take a strategic and proactive approach to information security, maintaining adequate staffexpertise, building in best practice controls and testing and updating these as the marketdevelops. Make active utilization of system based security management and monitoring tools.
• Ensure that crisis management processes are able to cope with internet related incidents.

One of the benefits that banks experience when using e-banking is increased user satisfaction. Thisdue to that users may access their accounts whenever, from anywhere, and they get involved more,this creating relationships with banks.Banks should provide their clients with convenience, meaning offering service through severaldistribution channels (ATM, Internet, physical branches) and have more functions available online. Otherbenefits are expanded product offerings and extended geographic reach. This means that banks can offer awider range

and newer services online to even more customers than possible before.The benefit which is driving most of the banks toward e-banking is the reduction of overall expenses. With e-bankingbanks can reduce their overall expenses in two ways: cost of processing transactions is minimized andthe numbers of branches that are required to service an equivalent number of customers are reduced.With all these benefits banks can obtain success on the financial market. But e-banking is a difficultbusiness and banks face a lot of challenges.

## 5. Reference:

1. Business Objects Learning Solution to Power e-Business Intelligence, Editura Business Objects,
2001
2. AFZENI PAOLO, STEFANO CERI, „Database Systems", Ed. McGraw-Hill, 1999.
3. AVERACE CHRISANTHI, TONY CARNFORD, „Developing Information Systems. Ideas,
Issues and Practice", Ed. Macmillan Press, 1993.
4. Adamson C. , Venerable M. Data Warehoutilization Design Solutions, Editura, Wiley, 1998
5. Berry J. A. M. , Linoff G. Data Mining Techniques: Marketing, Sales and Utilizationr Support,
Editura Wiley, 1997.

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

7. 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.

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

9. 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.

10. Internet Banking Comptroller's Handbook, 1999. Comptroller of the Currency Administrator of National Banks. October 1999, USA. James, A.N., 2005.