#WorldWide Readership ©Scholedge R&D Center

SCHOLEDGE INTERNATIONAL JOURNAL OF MANAGEMENT & DEVELOPMENT

Vol.2, Issue 7 ISSN 2394-3378 Archives available at http://thescholedge.org

BIOMETRIC RISKS- HOW TO DEAL WITH THE CHALLENGES

PRIYANKA GAUR[1], PRABHAT SRIVASTAVA[2*]

[1] Ph.D. Scholar, School of Business Management, Noida International University, Greater Noida, India

[2]Director, School of Business Management, Noida International University, Greater Noida, India

ABSTRACT

The advent of Internet has introduced our society with the security related threats, and after the introduction of IT Act 2000 these threats have entered and strongly infected the financial field. In addition to growing needs for speedy, accurate and reliable security, biometric technologies has been flaunted as the most potent technology in dealing with the identification and authentication issues. So in many countries nowadays biometric system has started to penetrate into financial sector. This paper presents a brief picture about all the threats associated with Biometrics when same is set up and is used for authenticating financial transactions. The paper reviews and incorporates the various studies associated with biometric system where the risks related to the technology is explored and discussed. The aim of the paper is to accustom us with the challenges which biometric technology will come across when same is implemented for authentication financial transactions. After analyzing various threats the study also suggests the ways of overcoming the risks related to the biometric technology.

KEY WORDS: Internet, Security, Threats, Financial, Biometric, Technology, Identification, Authentication, System, Transactions, Risks

1. INTRODUCTION

The number of frauds happening in the financial sector all around the world has been at an ascending rate so to overcome this issue last few decades in this sector has been under the process of nonstop expansion of liberalization and modernization in terms of initiating technological innovation. This is done to meet the growing need of providing secured monetary transaction to customers. Many global banks and financial institutes have found the solution in biometrics authentication system to cater the requirement of protected transaction.

The term biometrics is derived from the Greek words bio (life) and metric (to measure) (Scherer, 2005) [1]. Biometric identification exploits the universally recognized fact that certain physiological or behavioral characteristics reliably distinguish one person from another

(Scherer, Ahmed and Siyal, 2005) [2].

Biometric system is based on the fact that every person is unique and possesses distinctive characteristics and they can be identified and distinguished from one another with this.

The use of Biometrics has become a common practice in many areas for the purpose of identification of a human and there are a number of researches related to this aspect whereby the system identifies the human by his individual anatomy such as his fingerprints and voice (Venkatraman and Delpachitra. 2008).[3]
In short, biometric is the process of automatically recognizing a person using distinguishing traits not shared by any other individuals (Harris and Yen, 2002; Scherer, 2005). [4]
Biometrics system is based on identification of individuals by a physical or behavioral characteristic. Examples of recognition of physical characteristics are: fingerprints, iris, face or even hand geometry. Behavioral characteristic can be the voice, signature or other keystroke dynamics.

2. APPLICATION OF BIOMETRIC SYSTEM

Biometric system can be used in financial sector for following purposes

- Biometric system can be used as a replacement of identity card at retail outlets for expensive ornaments jewelry or other expensive shopping.
- Biometric system can be used in place of signature for any kind of payment either for cash withdrawal at biometric ATMs or for any kind of financial payments at retail outlets or at shopping malls.
- Identification purpose at the crime site.
- National identification for instance adhar card in India to remove the problem of multiple ID cards of a single individual.
- To rebate subsidy and other financial support provided by government for poor and needy people
- Used by bankers for authorizing financial transactions.
- After misfortunate incident of 9/11 in America, 26/11 in Mumbai and series of other terrorist attack all over the world it is now considered important to have unique identification of all individuals in a territory, for security of a country and its people. Therefore biometric is considered as a powerful means to combat such attacks and to identify and keep a check on the financial source of such unsocial group of the society.
- In India the government has decided to issue biometric PAN cards to taxpayers across the country [5] to weed out the problem of duplicate and fake ones.

3. RESEARCH METHODOLOGY

This research study adopts a qualitative approach where previous studies related to e-banking and biometrics were analyzed and discussed. This study is completely based on the literature review and the findings and suggestions were recommended based on the analysis of the literature review. Various studies related to biometrics in the past were considered and critically evaluated to develop the findings of the study in the context of the various risks associated with its implementation in financial sector.

4. RISK RELATED WITH BIOMETRIC PAYMENT SYSTEM

The days of paper work are now passé. These days all the monetary transactions are done online through internet. This has made the hackers and fraudster smarter and more vulnerable to carry out frauds. Security vulnerabilities are part of web reality. The success of internet, its low cost, global reach and flexibility has heaved the option of both opportunities and risks for the banks. At one point where internet facilitates banking customer with its anytime and anywhere banking service on the other hand internet attracts an increasing number of hackers and fraudsters to carry out their malicious intentions of making quick money.

4.1 STRATEGIC AND MANAGERIAL LEVEL PLANNING RISK

The global reach of internet has made it challenging for the management to provide a strong forceful identity management tools for authenticating online financial transactions. Collaborating with biometric technology for the same appears to be a promising solution, but to deploy this technology intelligently to meet the national and international security need in the financial sector is definitely a challenge.

A financial institution's board and management should therefore understand the strategic risk associated with biometric technology and at the same time before executing such services the resulting risks associated with it should also be evaluated. Inefficient planning and wrong investment decisions can enhance the company's strategic risks.

The strategic risks associated with biometrics are as follows:

- Biometric technology is still holds an unknown fear for the financial sector as it is still more theoretical based and lesser towards its practical application. So, the pros and cons of the technology is still not vastly tried and tested in the financial sector.
- All biometric systems work in similar ways, but it is important to remember that the ease of enrolment and quality of the template are critical success factors in the overall success of any biometric system [6].
- There are no particular biometrics which may successfully meet the requirements of all applications. A complete study on the application and higher probability of the biometric chosen to provide correct results should be considered before its installation.
- The physical harm to an individual that this technology can bring in should be considered. Concerns relating to actual harms can include physical harm to an individual from the sensor; for example, the laser used in retinal scanning, as well fear that an impostor might want to sever a limb, such as a finger, in order to bypass the biometrics system [7, 8].
- Another concern raised regarding working within the iris recognition industry is whether eye infections such as conjunctivitis are transferable by the camera. Users of the touch-based biometric scanners also often fear the transmission of illness and bacteria through the use of scanners [7, 8].
- Different countries have different cultures and religious beliefs which govern business and social practices, and people will be hesitant to adopt practices considered contrary to their cultural or religious dictates.[9]

Financial institutions should pay attention to the following to avoid strategic risks:

- The financial institutes at the foremost should launch comprehensive and broadly acknowledged standards for biometric information and biometric devices that captures the traits. The accepted standard should be capable enough to withstand the testing and analysis procedure for broadly accepted certification.
- The management on priority should always invest in the working of research and development of the technology to ensure that individual privacy and public confidence in biometric technology and systems is always maintained.
- Before introducing biometric in a particular financial institutes for verifying monetary transactions the management of the respective institute should be adequate enough to have a complete details of how far the biometrics has brought down the number of frauds happening in the institutes already using biometric technology for verification purposes.
- Adequacy of technical, operational, compliance, or marketing support to choose right type of biometric product and services that can be applied to meet the need of protected transactions from the available biometric options. Prabhakar, S., S. Pankanti, and A.K. Jain in their study on in their study on Biometrics Recognition: Security and Privacy Concerns have compared five biometric on seven different parameters. These parameters are –barriers to universality, distinctiveness, permanence,

collectability, performance, acceptability, potential for circumvention and "depending on the application's usage and the biometric characteristic's features we are able to suitably match a particular biometric to an application [7]"

- Adequacy of management to track how far the implementation of biometric technology has brought down the number of frauds happening in their own financial company.
- Costs involved in establishing biometric technology in their financial institutes for verification purposes.

  After choosing the right biometric its social acceptance of the technology should be considered. Many Christians, for example, believe biometrics represents the "Mark of the beast" as described in Revelation [7, 8] and this could result in prohibiting their use. In addition women's facial recognition would be prohibiting in some Muslim countries such as Saudi Arabia.
- After successful introduction of biometrics, the costs and availability of biometric companies to provide technical support for the enrolment, installation and other issues related to smooth working of biometric technology for secured financial transactions.
- Competitions among national and global financial institutions which are offering biometric verification for hassle free functioning of daily monetary transactions to attract customers.

4.2 FUNCTIONAL AND OPERATIONAL RISK

Operational risk has a strong alliance with the risks mentioned in association with financial transactions According to Peterson (2003) security is considered as the most influential factor when it comes to the acceptance of internet banking among the consumers. [10].The main benefit of online transactions is the facility of anytime and anywhere access, the very same reason has made it more vulnerable for fraudulent activities. There is an urgent need for a privacy and security policy to protect consumers' personal and financial information

The increased security and better operational risk management is the need of today's customer. Biometrics looks very promising in overcoming the risks associated with both retail and online banking but the very same technology is also susceptible to operational risks.

Biometrics is prone to following operational risks

- People these days spend a lot of time online and all the data is stored online which makes the biometric data more sensitive and the risk of identity swapping with criminal is more likely to happen.
- Wrong biometric updated on wrong ID card this operational risk is more probable to happen at the time of enrolment of biometric details.
- Risk of failure to enroll rate (FTER) or FER is the percentage of the population which fails to complete enrollment for a biometric solution or application. Failure can be due to physical differences, to lack of training, environmental conditions or ergonomic. [11]
- Risk of false match or acceptance rate (FMR or FAR).A false match occurs when a system incorrectly matches an identity, and FMR is the probability of individuals being wrongly matched. They may occur because there is a high degree of similarity between two individuals' characteristics.
- Risk of false non-match rate (FNMR) or false rejection rate (FRR). FNMR means mistaking two biometric measurements from the same individual to be from two different individuals [7].

Financial institutions should pay attention to the following to avoid operational risks:

- Use of multiple biometric techniques for execution of a single transaction to combat frauds.
- Systematized procedure for customer's falling in FTER category.
- Advance and appropriate system and technology for controlling FAR and FRR. loan

4.3 CREDIT AND LENDING RISK

A well organized biometric credit information system is required to control the number and amount of loan defaulters in the financial system. This biometric credit information system will record all the valuable information collected on borrowers. The system will record, store, maintain and update the credit information with the biometric details of the respective borrowers. Such information is accessible to all financial institutions and they can refer the same before granting the loan to a borrower. The past credit history and payment behavior of borrower will help these financial institutes in evaluating and making payment related decisions. This system and practice will lower the inaccurate credit risk assessment and will aware the lenders about the outstanding debt obligations of their clients. Customers will also have the benefit of considering various options for their credit related needs

The credit risk for both lenders and borrowers which biometric credit information system will bring in the financial sector is discussed below-

RISK FOR LENDERS

- Fear of competition and poaching of clients- The accurate data with complete credit profile of a customer may lead to consequently losing potential customers to competitors.
- All financial institutes may have monopoly in one or other loan products but this easy accessibility of customer information may result in losing monopoly developed from exclusive access to customer details even in their most promising and potential products therefore generating unanticipated loss for the lenders.
- Easy moving of customers from one lender to another may have an adverse effect on cost of credit and service.

RISK FOR BORROWERS

- Borrowers may not be happy with biometric data being shared – privacy concerns, higher risk of identity thefts.
- Borrowers not paying credit bills due to some kind of frauds might feel that their reputation and future eligibility and prospects for credit is hampered by some false negative data in biometric credit information system.

The financial institutes should pay attention to following to avoid credit risks:

- The financial institutes should have some provision to protect borrower's information
- The access of biometric credit information system should only be given to responsible high officials who are approving loans and not to every staff to control its misuse.
- The financial institutes should rigorously on security of the data on biometric credit information system so that the trust of the customer it has gained in the past years is sustained.
- The biometric credit information system should be capable enough to distinctly separate the fraudsters from non payers and potential payers

4.4 FUND MOBILITY AND REPUTATIONAL RISK

A poor transactional security will hamper the reputation of financial institutes. The trust that people have in financial institutes is more likely to boost as all their online and offline transactions can now only be executed after their biometric verification. This will surely enhance mobility of funds. The introduction of biometrics will amplify both number of transactions happening daily and the cost of transaction. The fund mobility which substantially increases the number of transactions happening daily could result in slower system speed and long transaction time. The higher transaction cost due biometric system can only be marginally adjusted with high number of transactions. The financial institutes should pay attention to following to avoid fund mobility and reputational risk:

- Financial institutes should invest on research and development of a full proof biometric system which gives no chance to hackers to act as authorized users.
- This will help financial institutes in gaining the trust of investors this will multiply investor's investment value in the company. Market capitalization is one of the most important characteristics that help the investor determine the returns and the risk in the share. A high value of market capitalization will therefore boost the trust of investors in the financial institute.

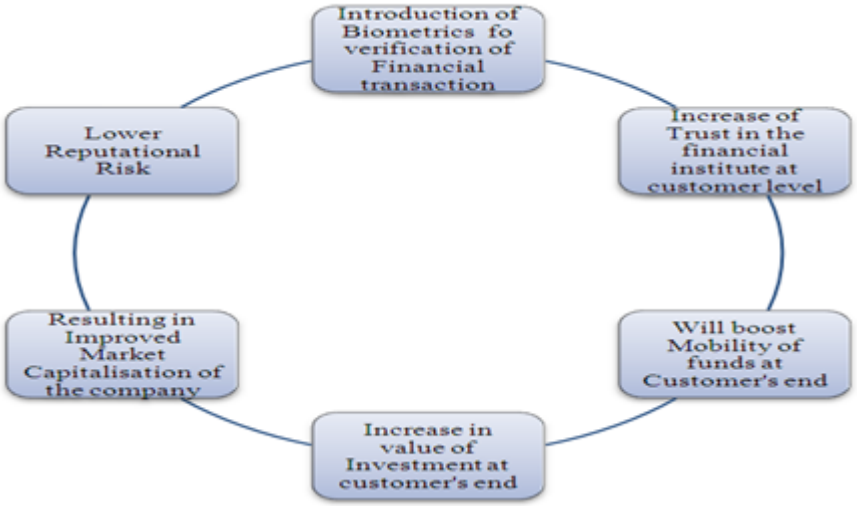

Diagram1. Shows relationship cycle of Biometrics, Trust, Fund Mobility and Investment, Market capitalization and Reputational Risk

- Fund mobility will help these institutes to potentially spread out and attain global reach.
- Mobility of fund will help in expansion of business and higher profit margins, increase in number of work and projects will in turn increase the job opportunities and better salary and incentives to the associated employees

4.5 Legal Risk – A proper legal frame work should be set up in advance before introduction of biometrics this will dissuade fraudulent activities of hackers. The research and development company should analyze the different legal issues that might pop up in future with the advent of biometrics.

5. RISKS MANAGEMENT PRINCIPLES

The following eight principles should be followed by the management before implementing biometrics in financial institutes

- Investment in research and development of biometrics.
- Launching a pilot plan before introducing it for public.
- Introducing different and appropriate biometrics for diverse products and services. A type of biometric useful in one product and service might not be useful in other.
- Ensure complete security and protection against unauthorized access
- Maintenance of customer's privacy and confidentiality of customer's information.
- Controlling the confidential data computer system from unauthorized and external access
- Focus on implementing multiple biometrics for a service to attain two tier security
- Not to compromise on lower cost and poor quality of biometric authentication system.

6. CONCLUSION

The current paper has elaborately explained the various risks associated with introduction of Biometrics in financial institutes. The different kinds of risks which a financial institute will come across are discussed in detail these risks are strategic and managerial planning risk, operational and functional risks, credit and lending risks, fund mobility and reputational risk and legal risk. The eight principles are also set which can be universally applied before the implementation of biometrics in any financial institutes.

REFERENCES

[1] Scherer, (2005). Retrieved from http://www.questia.com/library/1G1-267610935/adoption-of-biometric-technology-in-online-applications

[2] Scherer, Ahmed and Siyal, (2005). Retrieved from http://eprints.usm.my/25354/1/ADOPTION_OF_BIOMETRIC_TECHNOLOGY.pdf

[3] Venkatraman S and Delpachitra I.(2008) . " Biometrics in banking security: a case study" . Information Management & Computer Security, vol.16, no.4, pp415-430.

[4] Harris and Yen, (2002); Scherer, (2005). Retrieved from http://eprints.usm.my/25354/1/ADOPTION_OF_BIOMETRIC_TECHNOLOGY.pdf

[5] An article 'Govt to issue biometric PAN cards' from The Times of India (11April, 2011) Retrieved from http://timesofindia.indiatimes.com/business/india-business/Govt-to-issue-biometric-PAN-cards/articleshow/7945877.cms

[6] ALLAN, A., Biometric Authentication. Perspective. Gartner Research, 2002a: p. 1-31.

[7] Prabhakar, S., S. Pankanti, and A.K. Jain, Biometrics Recognition: Security and Privacy Concerns. IEEE Security & Privacy, 2003. 1(2): p. 33-42.

[8] Woodward, J.D., et al., Army Biometric Applications: Identifying and Addressing Sociocultural Concerns. 2001: RAND.

[9] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala, Secure Biometrics Authentication: A brief review of the Literature retrieved from http://www.scribd.com/doc/23874642/Secure-Biometrics-Authentication-A-brief-review-of-the-Literature#scribd

[10] Ahmad, D.T., & Hariri, M. (July, 2012). User Acceptance of Biometrics in E-banking to improve Security, Business Management Dynamics Vol.2, No.1, Jul 2012, pp.01-04 Retrieved from bmdynamics.com/issue_pdf/bmd1102400104.pdf

[11] http://www.biometric-solutions.com/glossary.php?term=Failure%20to%20Enroll%20Rate