The Seybold Report

ISSN 1533-9211

10.5281/zenodo.6617007

E-BANKING AND FRAUDULENT ACTIVITIES IN BANGLADESH: COMBATING BY INTEGRATION OF TECHNOLOGY

SHAHJADY SULTANA,
PhD Aspirant, Limkokwing University of Creative Technology

A.K.M. SHAFIQUR RAHMAN,
Senior Assistant Professor, BGMEA University of Fashion & Technology, Bangladesh

ABU YUSUF MOHAMMAD HABIBUR RAHMAN MCIM,
The Chartered Institute of Marketing

JOBAER MIAH,
Student of IBA, University of Rajshahi, Bangladesh

Abstract

Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. With the rapidly growing banking industry globally, frauds are increasing fast, and fraudsters have started using innovative methods. Shockingly, the banking industry in everywhere dubs rising fraud as an inevitable cost of business. One of the most challenging aspects in the banking sector is to make banking transactions free from electronic crime. There is no "one silver bullet" to stop all frauds forever. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

Keywords: Bank frauds, banking industry, risk management, use of technology, current scenario, future challenges.

1. Introduction

It is universally accepted that for the smooth functioning of a money market and economic growth of a country, an efficient and good banking system is a must. Banking industry in India has traversed a long-way to assume its present stature in the21st century. Unfortunately, it is also true banking industry has to face many types of frauds and scams. The Reserve Bank of Bangladesh (RBB) is the central policy making and national level regulatory body by keeping an eye over the entire banking industry.

Fraudulent activities cause losses to banks and their customers, and also reduce money available for the development of economy. Shockingly, "the banking industry in Bangladesh dubs rising fraud as an inevitable cost of business" (E&Y). According to Bangladesh Banking Fraud Survey Report (Edition II, 2015), "Common causes of frauds in banking include diversion & siphoning of funds, whereas fraudulent documentation and absence, or overvaluation of collaterals were the main reasons for fraud in retail banking." Thus, in nutshell, "inadequate measures to prevent banking fraud is the primary reason for widespread

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

frauds. Technology is like a double-edged sword, which can be used to perpetuate, detect and prevent frauds."

However, Gates and Jacob (2009) have pointed out that "the misuse of technology in the banking includes use of banking access for over-payments to vendors, sharing confidential information, and misuse of technology for unauthorized activities." Also, providing services on mobile and social media platforms, with limited knowledge of security requirements, poses lot of threats to customers and banks. Data analysis software enables auditors and fraud examiners to analyze an organization's business data to gain insight into how well internal controls are operating and to identify transactions that indicate fraudulent activity or the heightened risk of fraud. Bhasin, M.L. (2016)

Data analysis can be applied to just about anywhere in an organization where electronic transactions are recorded and stored. Use of new technology can prove to be very helpful to control the fraud risk in banks (Kumar, V. and Sriganga, B.K. (2014)." It is a well-known fact that investigation and prosecution of fraudsters in Bangladesh is "very slow, time-consuming process, thus, the danger of fraud will always be there. Since banking industry is a highly-regulated industry, there are also a number of external compliance requirements that banks must adhere to in the combat movement against fraudulent and criminal activity.
Recently, banking sector business has become more complex with the development in the field of information and communication technology, which has changed the nature of bank fraud and fraudulent practices. For example, Berney, L. (2008) observed that customers rely heavily on the web for their banking business, which leads to an increase in the number of online transactions. Similarly, Gates, T. and Jacob, K. (2009) and Malphrus, S. (2009) have asserted that the internet provides fraudsters with more opportunities to attack customers, who are not physically present on the web to authenticate transactions.

Fraud, however, is a major component of operational risk. But if the banker is upright and knows his job well, the task of the defrauder will become extremely difficult, if not impossible. This has thrust enormous responsibilities in terms of prescribing and maintaining an effective architecture of internal checks and controls, and optimum use of innovative technology (Wells, J. T. (2005). Banks have more technology and more incentive than ever to combat fraud in electronic banking services. But whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful.

1.1 Meaning and Types of Bank Frauds

Fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. As per RBB, fraud can be "loosely" described as "any behavior by which one person intends to gain a dishonest advantage over another." Fraud encompasses a wide-range of illicit practices and illegal acts involving intentional deception or misrepresentation. The Institute

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

of Internal Auditor "International Professional Practices Framework (IPPF)" defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force.

Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, therefore, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation.

Banks can secure and preserve the safety, integrity and authenticity of the transactions by employing multipoint scrutiny: cryptographic check hurdles. In addition, banks should rotate the services of the persons working on sensitive seats, keep strict vigil of the working, update the technologies employed periodically, and engage more than one person in large-value transactions. Of course, internal auditors can continue to win the battle against frauds and scams through the continued application of fundamentals, such as education, technological proficiency, and support of good management practices.

Close attention and vigilance on the part of both banks and customers is, therefore, the best deterrence. According to Freddie Mac (2015), "Fraud Mitigation Best Practices" include: (a) Fraud Risk Management Policies and Procedures: Put sound and appropriate fraud detection, prevention, investigation, resolution, and reporting policies and procedures in place, and communicate them to employees; (b) Regulatory Compliance: Ensure appropriate policies and procedures are in place pertaining to company's obligations under the RBB Act, as applicable; (c) Ethical Conduct: Familiarize employees with your company's standards for ethical conduct; (d) New Employee Awareness: Incorporate fraud awareness in new employee orientation programs; and (e) Training: Ensure that employees receive fraud training appropriate for their roles and levels.

One of the most challenging aspects in the Bangladeshi banking sector is to make banking transactions free from electronic crime. Fraud detection in banking is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike. It may be noted at the outset that all the major operational areas in banking industry offers a good opportunity for fraudsters, with growing fraud and financial malpractices being reported under deposit, loan, and inter-branch accounting transactions (including remittances).

Frauds generally take place in a financial system when safeguards and procedural controls are inadequate, or when they are not scrupulously adhered to, thus, leaving the system

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

vulnerable to the perpetrators. Most of the time, it is difficult to detect frauds well-in-time, and even more difficult to book the offenders because of intricate and lengthy legal requirements and processes. In the fear of damaging the banks reputation, these kinds of incidence are often not brought to light. Historical evidence shows that whether the agency (or individual) committing the fraud works for the bank or deals with it, the culprit usually does very careful and detailed planning before he finally attacks the system at its most vulnerable point.

In today's volatile economic environment, the opportunity and incentive to commit frauds have both increased. Instances of as set misappropriation, money laundering, cybercrime and accounting fraud are only increasing day-by-day. With changes in technology, frauds have taken the shape and modalities of organized crime, deploying increasingly sophisticated and innovative methods of perpetration. In the 21st century, as financial transactions become increasingly technology-driven, new technology seems to have become the weapon of choice, when it comes to fraudsters.

According to the PwC (2014) Global Economic Crime Survey 2014, "cybercrime was one of the top economic crimes reported by organizations across the world, including Bangladesh." Regulations and laws governing the financial services sector in Bangladesh are continuously evolving. For any growing organization, it is critical to keep up with the changing laws in order to mitigate risks and stay ahead. Some of the important regulatory drivers for the financial sector in Bangladesh are as follows: (a) Reserve Bank of Bangladesh Act, 1934; (b) Securities and Exchange Board of India Act, 1992; (c) Companies Act, 2013; (d) Prevention of Money Laundering Act, 2002; and (e) The Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015. The PwC's Survey identified that suspicious transaction reporting, effective fraud risk management measures, whistle blowing processes and tip-offs helped financial services organizations to detect most frauds.

There is no simple way to squash fraud, but by implementing the right mix of technologies and prevention techniques, treasury executives can greatly reduce their organization's risk. As Accenture's Santoro puts it, "A solid portfolio of solutions with multiple layers of protection and controls can go a long way toward providing the necessary protection. If you put enough deadbolts at the door, thieves are going to give up and look elsewhere." It is an endless game of "cat and mouse" between banks and cyber-criminals.

There is a virtual arms race taking place online between financial institutions and cyber criminals, who as soon as the bank deploys a new process or technology to prevent online fraud, they find a weakness to exploit. In addition, customers expect to be protected from fraud, but also want anti-fraud tools to look at them holistically, assessing the fraud risk of transactions based on their individual profiles. Five ways to combat bank frauds are highlighted below as:

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

(a) Adopt appropriate technologies: An inclusive mix of strong authentication systems; analytics software; and bank services, positive pay and payee verification, for example, can greatly reduce an organization's exposure to fraud. It is important to have layers of protection.

(b) Beef up your internal controls: Sarbanes- Oxley mandates that companies pay strict attention to their internal controls. But even the most thorough Sarbanes-Oxley compliance effort cannot provide comprehensive protection against fraud. Proactive organizations will want to put additional controls in place, including rigorous approval procedures and careful separation of duties. That is especially true of disbursement processes, such as wire transfers.

(c) Screen job applicants carefully: One of the biggest security problems company's face is fraud perpetrated by trusted insiders. Key finance functions such as treasury must conduct background checks on potential hires, and companies should also consider drug testing and honesty testing. It is the first line of defense.

(d) Educating workforce: Employees need to understand how damaging fraud can be to the organization. They must be able to recognize signs of fraudulent activity and know how to report it. In addition, treasury employees will need to be trained in the correct use of the company's fraud protection tools and technologies.

(e) Prosecute thieves: Many organizations fire employees who are caught stealing but avoid prosecuting them for fear of bad publicity. A zero-tolerance policy goes a long way toward reducing the risk of illegal activity. Likewise, managers should immediately turn over any evidence of suspected fraud to law enforcement agencies.

1.2 Who is Responsible for Fraud Detection?

While the senior management and the board of Directors of the Banks are ultimately responsible for a fraud management program, internal audit can be a key player in helping to address fraud. By providing an evaluation on the potential for the occurrence of fraud, internal audit can show an organization how it is prepared for and is managing these fraud risks. Instead of relying on reactive measures like whistleblowers, organizations can and should take a more hands-on approach to fraud detection. A fraud detection and prevention program should include a range of approaches–from point-in-time to recurring and, ultimately, continually for those areas where the risk of fraud warrants.

Based on key risk indicators, point-in-time (or ad hoc) testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered. In today's automated world, many business processes depend on the use of technology. This allows for people committing fraud to exploit weaknesses in security, controls or oversight in business applications to perpetrate their crimes.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

However, the good news is that technology can also be a means of combating fraud. Internal audit needs to view technology as a necessary part of their toolkit that can help to prevent and detect fraud. Leveraging technology to implement continuous fraud prevention programs helps to safeguard organizations from the risk of fraud and reduce the time it takes to uncover fraudulent activity. This helps both to catch fraud faster and to minimize the impact it can have on organizations. According to ACL,11 the analytical techniques, which may prove very effective in detecting fraud, are shown below:

- Calculation of statistical parameters to identify outliers that could indicate fraud
- Classification to find patterns amongst data elements
- Stratification of numbers to identify unusual entries
- Digital analysis using Benford's Law to identify unexpected occurrences of digits in naturally occurring data sets.
- Joining different diverse sources to identify matching values where they should not exist
- Duplicate testing to identify duplicate transactions such as payments, claims or expense report items.
- Gap testing to identify missing values in sequential data where there should be none.
- Summing of numeric values to identify control totals that may have been falsified
- Validating entry dates to identify suspicious items for postings or data entry.

As very strongly emphasized by Bhasin, M.L. (2015) "In the 21st century, the forensic accountants are in great demand and forensic accounting is listed among the top- 20 careers of the future." Recent accounting scandals and the resultant outcry for transparency and honesty in reporting, therefore, have given rise to two disparate yet logical outcomes. First, forensic accounting skills have become very crucial in untangling the complicated accounting maneuvers' that have obfuscated financial statements. Second, public demand for change and subsequent regulatory action has transformed corporate governance (CG) scenario.

Therefore, many senior-level company officers and directors are under the ethical and legal scrutiny. In fact, both these trends have the common goal of addressing the investors' concerns about the transparent financial reporting system. The failure of the corporate communication structure has also made the financial community realize that there is a great need for skilled professionals that can identify, expose, and prevent structural weaknesses in three key areas: poor CG, flawed internal controls, and fraudulent financial statements. Therefore, forensic accounting skills are becoming increasingly relied upon within a corporate reporting system that emphasizes its accountability and responsibility to stakeholders.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

2. Review of Literature

Jeffords, R.; Marchant, M. L. and. Bridendall, P.H. (1992) examined 910 cases submitted to the "Internal Auditor" during the nine-year period from 1981-1989 to assess the specific risk factors cited in the Treadway Commission Report. Approximately 63 percent of the 910 cases are classified under the internal control risks. Similarly, Calderon, T. and Green, B.P. (1994) made an analysis of 114 actual cases of corporate fraud published in the "Internal Auditor" from 1986 to 1990. They found that limited separation of duties, false documentation, and inadequate or nonexistent control account for 60 percent of the fraud cases. Moreover, the study found that professional and managerial employees were involved in 45% of the cases. Ziegenfuss, D.E. (1996) performed a study to determine the amount and type of fraud occurring in state and local government.

Willson, R. (2006) examined the causes that led to the breakdown of 'Barring' Bank, in his case study, "the collapse of Barring Banks". The collapse resulted due to the failures in management, financial and operational controls. However, Bhasin, M.L. (2013) examined the reasons for check frauds, the magnitude of frauds in Bangladeshi banks, and the manner in which the expertise of internal auditors can be integrated in order to detect and prevent frauds in banks. In addition to considering the common types of fraud signals, auditors can take several 'proactive' steps to combat frauds. One important challenge for banks, therefore, is the examination of new technology applications for control and security issues

Mhamane, S. and Lobo, L.M.R.J. (2012) in their study attempted to detect and prevent fraud in case of internet banking using Hidden Markov Model algorithm. Chiezy and Onu7 evaluated the impact of fraud and fraudulent practices on the performance of 24 banks in Nigeria during 2001-2011. Secondary sources of data were used for the study. The relationship between fraud cases and other variables were estimated using Pearson product moment correlation and multiple regression analysis was used. The paper recommended that banks in Nigeria need to strengthen their internal control systems and the regulatory bodies should improve their supervisory role.

However, Dzomira, S. (2014) investigated the use of digital analytical tools and technologies in electronic fraud and detection used in the Zimbabwe banking industry. He concluded that banking institutions should reshape their anti-fraud strategies to be effective by considering frauds detection efforts using advanced analytics and related tools, software and application to get more efficient oversight. Similarly, Kumar, V. and Sriganga, B.K. (2014) highlighted the common insider frauds occurring in banks and also tried to categorize them into different types. They focused on different generic data mining techniques and in specific, the techniques used for detecting insider frauds.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

3. Research Methodology

The present study is both descriptive and analytical in nature. As part of the study, a questionnaire-based survey was conducted among 200 bank employees of the capital city Dhaka area. The questionnaire was structured into two parts. In fact, the first part comprised of several questions that attempted to know their opinions while working in a bank regarding training received, attitude towards the procedures, awareness level towards frauds and their compliance level under the following six heads: deposit account, loans and advances, administration of passbook and check book, drafts section, internal and inter-branch accounts, and credit-card section.

Moreover, the second part encompassed the issues about how to integrate technology in the banking industry in order to detect and prevent frauds in Bangladeshi banks. It also examined the technology solutions available and how to integrate forensic approach to combat bank frauds in the Bangladeshi banking industry.

All the respondents were selected through the random sampling method. There were 30 private sector banks in the area and finally, 21 banks were selected. The sampled employees comprising of Managers, Officers and Clerks of the branches were given the questionnaire by personally visiting them in bank. Out of all the employees, 170 employees responded, with an overall response rate of 85%. In all, there were 40 managers, 120 officers and 10 clerks as respondents.

4. Findings and Analysis of Data

In the first part of the questionnaire, we focused on the compliance level of these security controls were measured under the following six heads—internal checks, deposit accounts, administration of check books and passbooks, loans and advances, drafts, internal accounts and inter branch accounts. The results of this study indicate that the security control measures are not fully complied with. As per a study, limited separation of duties, false documentation, and inadequate or nonexistent control account for 60% of the fraud cases. It found that professional and managerial employees were involved in 45% of the cases. Thus, education, training and awareness programs are informal intervention measures that should be implemented to prevent frauds.

Discussion on frauds cannot be complete without analysis of human behavior. An employee in a bank is like a fish in a small ocean. Nobody can determine when and how much water a fish has consumed. Likewise, a corrupt and dishonest person in a bank can commit frauds with impunity. Unfortunately, most of the employees committing frauds get scot free, with the award of minor penalties, and the cases pending in courts keep on dragging for many years. Study shows that “detection of fraud takes very long-time, and banks tend to report an

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

account as fraud only when they exhaust the chances of recovery. Delays in reporting of frauds further delay the alerting of other banks about the modus operandi through caution advices that may result in similar frauds being perpetrated elsewhere."

Bhasin concluded "In the current environment, forensic accountants are in great demand for their accounting, auditing, legal, and investigative skills in order to detect and prevent frauds and scams in the Bangladeshi banking sector." An analysis of big cases looked into by the CBB (Central Bank of Bangladesh) reveals that bankers sometimes exceed their discretionary powers, and give loans to unscrupulous borrowers on fake/forged documents. There is lack of trained and experienced bank staff, and tremendous increase in banking business. By-and-large, new recruits do not have adequate training or experience before they are put into a responsible position. Undoubtedly, training improves the capabilities of employees by enhancing their skills, knowledge and commitment towards their work.

Moreover, bank staff feels they are overburdened with work. The life has become fast and the bank staff does not have enough time to scrutinize documents thoroughly. Dilution of system and no adherence to procedures is also a significant reason for bank frauds. This shows that a full-proof system has not been developed and implemented to familiarize the bank employees of various types of frauds that take place in banks every year. "Most banks try to put in place robust systems and controls to prevent fraud and forgery— regrettably crooks and criminals use more and more sophisticated methods, especially where online fraud is concerned.

The primary responsibility for preventing frauds lies with individual banks. Major cause for perpetration of fraud is laxity in observance in laid down system and procedures by supervising staff.

How Technology is shaping the Fight Against Bank Frauds?

Technology is like a double-edged sword. On the one hand, perpetrators are using it to further fraudulent schemes; on the other hand, we are making some of our best progress using the same technology. Undoubtedly, technology can prove helpful in fraud detection and prevention in banks. Unfortunately, the fraud takes on many forms to be handled with any 'single' application or approach. The cat and mouse game will continue. As technology becomes more advanced, fraudulent schemes will become more complex, while more sophisticated fraud solutions will be developed to combat hackers' best efforts.

As the landscape of fraud continues to shift, business leaders must be aware of trends and predictions that will allow them to implement internal/external controls and systems to help reduce the risk of fraud and keep them from becoming another statistic. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

Neural Networks have been extensively put to use in the areas of banking, finance and insurance. Usually, such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends. Fraud cases are statistically analyzed to derive out relationships among input data and values for certain key parameters in order to understand the various patterns of fraud. This knowledge of fraud trends is then iteratively taught to feedforward neural networks, which can successfully identify similar fraud cases occurring in the future.

In the realm of fraud detection, the ability to reveal relationships, transactions, locations and patterns can make the difference between uncovering a fraud scheme at an early stage as opposed to having it grow into a major incident. From money laundering schemes to anti-corruption laws, from manipulating financial statements by reporting fictitious revenues to inappropriate sanctioning; forensic analytical tools can help explore data and quickly identify errors, irregularities and suspicious transactions embedded within your business, thereby providing clarity to concerns raised by managers and employees.

Whether it is financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the banking sector. Most banks are, therefore, insisting on cashless and paperless transactions. The substantially larger proportion of technology related frauds in the Bangladeshi banking sector by number is only expected as there has been a remarkable shift in the service delivery model with greater technology integration in the banking industry. Even though the incidence of cyber frauds is extremely high, the actual amount involved is generally very low.

The new technologies adopted by banks are making them increasingly vulnerable to various risks, such as, phishing, identity theft, cards kimming, vishing (voicemail), SMSishing (text messages), Whaling (targeted phising on high net worth individuals), viruses and Trojans, spyware and adware, social engineering. Changing technology and rapid flow of information have placed the customer at the center. It is critical for every bank to understand customer needs and expectations and offer customized services.

While some of the risks in the banking sector have always been there, they keep on changing with the constantly evolving technology standards and regulatory framework. Part of the challenge is that the types of financial fraud and characteristics of fraudsters have changed in recent years. For instance, check fraud is in decline while electronic fraud is on the rise, and the latter tends to be perpetrated by more sophisticated criminals. Cheque fraud has been around the globe since the ancient time, but the pace of changing schemes has been very slow for banks to react with very good procedures—many of them still ‘manual’.

According to Bhasin “Some of the technological innovations, which may be already in use in some banks are: (a) Two-dimensional Bar Codes, (b) Data Glyphs, (c) Biometrics, (d) Cheque Image Processing, (e) Data Mining (f) Data Analytics, etc.” Given this complicated

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

fraud prevention picture, banks will need to figure out their own patterns of exposure and deploy tools with the best fit. Banks have more technology and more incentive than ever to combat fraud in electronic banking services. But whether they have enough technology and incentive to protect consumers from the headaches of a compromised account, payment card or identity is doubtful. Threats are escalating more quickly than what banks, or even just other businesses in general, can deploy in terms of defenses against those threats.

There is no "one silver bullet" to stop all frauds forever. Rather, the pace of new threats is not going to slow down and nobody (no bank, no retailer and no consumer) is ever 100% secured. What is needed instead is a combination of checks from a layered approach that banks will have to adopt and consumers will have to accept if they want to utilize electronic banking services. That suggests consumers should expect to see, and might want to welcome, an ongoing stream of new solutions that banks will employ to stay a step ahead of electronic banking fraudsters.

It is most unfortunate that the current system of usernames and passwords, with which consumers are familiar, is basically broken. Consequently, banks also have begun to deploy an array of other technologies, some of which are so exotic and sophisticated they might seem like science fiction. Here, is a summary of some of the technology that is on tap:

• **Device fingerprinting** tracks a series of identifiable hardware and software attributes to recognize a user's (or fraudster's) device.

• **Behavioral analytics** monitor navigation techniques and other aspects of a user's online behavior to search for anomalies or suspicious activity.

• **Malware detection** searches for potentially fraudulent changes to a user's Web browser to assess whether it's been compromised.

• **Knowledge-based authentication** presents a series of static or dynamic and supposedly secret questions to establish a user's identity.

• **Password tokens** give a user a one-time only password that must be entered before it expires.

• **Out-of-band authentication** challenges a user to access a one-time-only password or code that is sent to another device, such as a mobile phone or land line.

• **Transaction signing** requires a user to digitally sign each transaction.

• **Endpoint protection** requires a user to download a one-time-only, secure browser to access a website.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

• **Voice printing** records attributes of a caller's speech over time and matches those attributes against subsequent calls. Voice printing is an example of biometrics, which use unique physical traits, or characteristics to identify individuals.

However, as technology advances, we are seeing a distinct proliferation of more complex fraud schemes. At the same time, we are seeing more breakthroughs in the use of technology to detect fraud. Strategies that we have used in just the past few years will become completely outdated, as a fresh set of tactics will debut. To minimize the potential damage of fraud, companies need to invest not just in more advanced technology but in people and policies for detecting attacks as quickly as possible.

While the networks are just too large to prevent every attack from occurring, detection is crucial. Most companies do not have adequate protocols and staff in place to deal with incidents of fraud. While advanced technology serves as a great tool to combat fraud, the issue should be viewed as more than just an IT problem and looked at as a business problem. Remember, the cost of trying to prevent fraud is far less expensive to a business than the cost of fraud committed on a business.

5. Conclusion

While the banking industry in Bangladesh has witnessed a steady growth in its total business and profits, the amount involved in bank frauds has also been on the rise. This unhealthy development in the banking sector produces not only losses to the banks but also affects their credibility adversely.

The top three fraud risks that are currently the highest concern to the banks are: (a) Internet banking and ATM fraud, (b) E-banking (credit card and debit card, etc.), and (c) Identity fraud. Despite the proliferation of online and mobile service offerings and the rise in cybercrime, banks and financial institutions can fight back. A comprehensive anti-fraud program can not only protect customers but can cause would be cyber criminals to turn their attentions elsewhere.

It is important to understand that fraud investigation requires specific skill sets like forensic accounting and technology to collect adequate evidence. While the evidence unearthed by a fraud investigation can vary on a case-to-case basis; typically, it needs to be relevant and comprehensive to be admissible in a court of law. Certain additional aspects, such as, the source of the evidence, a legitimate witness, electronic evidence and data etc., can all add credibility to the case. In the absence of these, banks may not have the confidence to take legal recourse or action on the fraudster which could be one of the reasons why banks may not be reporting all the cases to law enforcement agencies.

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

Last, but not the least, effective customer education and communications programs–helping customers recognize how to prevent fraud, but also helping them understand their own responsibilities–should go hand-in-hand with sophisticated cyber security measures. Only by working in partnership with their customers can financial institutions develop truly effective fraud prevention efforts

References

Al-Amin S and Rahman S, Application of Electronic Banking in Bangladesh: An Overview, Bangladesh Research Publication Journal. 4(2), 172-184 (2010).
Graven M P, Electronic money. *PC* Magazine, 8 August, (2000).

Salehi M, Ali M and Zhila A., Islamic Banking Practice and Satisfaction: Empirical Evidence from Iran. ACRM Journal of Business and Management, Research. 3(2), 35-41(2008).

Cronin M J, Banking and Finance on the Internet. John Wiley and Sons (1997).

Chavan J, Internet Banking-Benefits and Challenges in an Emerging Economy. International Journal of Research in Business Management, 1(1), 19-26 (2013).

Nattakant U, Online Banking Users in Western Australian of Phishing Attacks"P. hd Thesis, Faculty of Computing, Health and Science, Edith Cowan University, (2012).

Biswas Set. al., Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges. Canadian Journal on Scientific and Industrial Research. 2(5), (2011).

Wysopal C, Eng C, Static Detection of Application Backdoors". Veracode. (2015).

Islam MM, Proposed ICT Infrastructure for E-banking in Bangladesh. Department of Computer and Systems Sciences, Royal Institute of Technology (KTH), Stockholm, Sweden (2005).

Parker D B, Fighting Computer Crime: A New Framework for Protecting Information. New York: *John Wiley & Sons*, Inc., (1998).

M. I. Khalil, I. Ahmad and M. D. H. Khan (2003) "Internet Banking: Development and Prospects in Bangladesh". "Internship report on E-banking in Southeast Bank ltd." available[online] http://bba-mba-arena.blogspot.com/p/internshipreports_06.html; Accessed on April 15th, 2012. G.P. Schneider (2010) "Electronic Commerce".

M.T. Fordney, L.L. French and J.J. Follis (2007) "Administrative Medical Assisting" Sixth Edition. http://en.wikipedia.org/wiki/Automated_teller_machine, accessed on march 20, 2012

S. Padmalatha (2011) "management of banking and financial services" Second edition. "E-Commerce-in-Bangladesh" available [online] http://www.scribd.com/doc/40520136/E-Commerce-inBangladesh#archive; Accessed on April 15th, 2012. B. Welch (1999) "Electronic Banking and Treasury Security"

M. Shah and S. Clarke (2009) "E-Banking Management: Issues, Solutions, and Strategies"

M. A. H. Mia, M. A. Rahman and M. M. Uddin (2007) "E-Banking: Evolution, Status and Prospects", The Cost and Management, 35(1): 36-48 January-February, 2007.

J. Yang and K.T. Ahmed (2009) "Recent trends and developments in e-banking in an underdeveloped nation – an empirical study" Int. J. Electronic Finance, 3(2) pp 115-132.

M. M. Islam (2005) "Proposed ICT infrastructure for E-banking in Bangladesh" Royal Institute of Technology (KTH) SecLab Department of Computer and Systems Sciences (DSV). Stockholm, Sweden, submitted in March

The Seybold Report
ISSN 1533-9211
10.5281/zenodo.6617007

6, 2005. E-Banking Features, Problems, Hacking and Solutions. Available [online] http://onlinebdinfo.blogspot.com/2010/12/ebanking-features.html; Accessed on April 15th, 2012.

H. M. Saidul Hasan, M A. Baten, A. A. Kamil and S. Parveen (2010) "Adoption of e-banking in Bangladesh: An exploratory study" African Journal of Business Management, 4(13) pp 2718-2727, 4 October, 2010.

M. M. Ali, R. Ahmed, A. Rahman and M. M. Azam (2007) "Electronic Banking in Bangladesh: Potential and Constraints" D. U. Journal of Marketing, 10, June 2007.

Dr. S. Biswas, A. Taleb and S. S. Shinwary (2011) "Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges" Canadian Journal on Scientific and Industrial Research 2(5) pp 181-194 May 2011.

N. Hossain (2000) "E-Commerce in Bangladesh: Status, Potential and Constraints" A report prepared for JOBS/IRIS Program of USAID.

M. M. Ali (2010) "E-Business and on line banking in Bangladesh: An Analysis" AIUB business and economics working papers series, 03, 2010.

M. A. Baten, and A. A. Kamil (2010) "E-Banking of Economic Prospects in Bangladesh" Journal of Internet Banking and Commerce, 15(2), August 2010.

M. A. Hossain, "E-Banking for Bangladesh perspective and legal remedy" Available [online] http://wwwlawlib.wlu.edu/lexopus/works/411-1.pdf; Accessed on April 23th, 2012.

S. Al-Amin and SK. S. Rahman (2010) "Application of electronic banking in Bangladesh: an overview" Bangladesh research publication journal, 4(2) pp 172-184, July-August, 2010.

M.A. R. Khan and M. M. Karim (2008) "E-banking and extended risks: How to deal with the challenge?"

S.M. S. Ahmed, Shah Johir Rayhan, Md. Ariful Islam and Samina Mahjabin (2012) "Problems and prospects of mobile banking in Bangladesh" International Refereed Research Journal, 3(1) pp 47-58, Jan. 2012.

M. A. Mthembu (2010) "Electronic Funds Transfer: Exploring the Difficulties of Security" Journal of International Commercial Law and Technology, 5(4), pp 201-205.

Legislation

The Banking Companies Act, 1991. Sec 12

The Information & Communication Technology Act, 2006. Sec 1 (4)

The Information & Communication Technology Act, 2006. Sec 1 (14)

The Information & Communication Technology Act, 2006. Sec 1 (1)

The Banking Companies Act, 1991. Sec 57

Information and Communication Technology Act, 2006, Sec 54

The Penal Code, 1860, Section 204

The Penal Code 1860, Section 441

Information and Communication Technology Act, 2006, Sec 56

Ibid, Section 447