Chapter – 2

LITERATURE SURVEY
Chapter – 2

LITERATURE SURVEY

2.0 Introduction

The literature survey is required to elicit the information connected with security of credit/debit card holder’s data. The researcher in view of topic “adoption of security standards in banks issuing credit/debit cards” has referenced the books, journals, magazines, periodicals, reports and relevant information was collected and compiled. The summary of researched materials was classified according to cyber frauds, e-banking, e-payment, security standards and credit/debit card and glossary of technical words developed.

2.1 Literature Survey Glossary

E-frauds(Cyber frauds)

According Macmillan Dictionary e-fraud is defined as “The activity getting/ obtaining money illegally using internet”. Interchangeably cyber fraud is also being used for e-fraud.

Identity theft

Identity theft, also known as ID theft is a crime in which a criminal obtains key pieces of personal information, such as social security /UID number or driver's license number, in order to pose as someone else.

Phishing (fish’ing) (n.)

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords, credit card, and bank account numbers that the legitimate organization already has. The web site, however, is bogus and created only to steal the user’s information.
E-banking (Internet banking)

The remote delivery of new and traditional banking products and services through electronic delivery channels.

Virus

A computer virus is a software program, script, or macro designed to infect, destroy, modify, or cause other problems within the computer or software programs.

Cyber Security Standards

Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.

E-payment

E-payment is a subset of an e-commerce transaction to include electronic payment for buying and selling goods or services offered through the internet.

The term 'electronic payment' is a collective phrase for different kinds of electronic payment methods available (also meaning online payment), and the processing of transactions and their application within online merchants and ecommerce websites.

Botnet and Zombie

A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source. The botnet may refer to a legitimate network of several computers that share program processing amongst them.

Usually though, when people talk about botnets, they are talking about a group of computers infected with the malicious kind of robot software, the bots, which present a security threat to the computer owner. Once the robot software (also known as malicious software or malware) has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander.
2.2 Classification of Literature Survey

The literature survey on the subject may be classified into following:

- E-frauds (Cyber fraud)
- E-banking (Internet banking)
- E-payments
- E-security
- Security standards

The literature consists of articles from journal, IT magazines and regulatory bodies reports giving the insight into various aspects of e-banking and e-security in the world of computers in particular, in the banking environment.

2.3 Literature Survey of Cyber Fraud (E-frauds)


While many label hackers as being malicious, evil, and destructive (and no doubt some are), Ms. Denning argues that on the whole, they are upstanding and considerate people who actually contribute to the well being of cyberspace. In many ways they see themselves as defending the citizen's right to expression and access to information. Their activities are done in harmless fun and they are careful not to inflict harm if at all possible. Hackers are bright and sophisticated computer experts who are out for a challenge and a thrill. If anything, they are useful in exposing the weaknesses of computer networks, and are indeed employed by business to test the security of their systems.


This site is also interested in defining types of cyber crime and nicely covers areas not addressed by the previous site. Real life examples of cases are highlighted. The site gives particular attention to the "lawless" nature of the internet. Here, it appears that the only form of governance is found in the self-regulating norms of the virtual community. Law enforcement on the net is
hindered by legal ambiguity and jurisdictional differences. References and links are provided for further study.


This is a lengthy and comprehensive report put forth by the United States Justice Department that examines the phenomenon of internet crime. Legal issues are discussed along with the challenges faced by law enforcement. The need for public awareness and education is stressed. A table of contents is provided (including appendices on specific types of cybercrime).

An international accounting and consulting firm conducted a global survey on e-fraud and its impact upon business (2000).

The survey, conducted every two years, is designed to raise awareness of the threat of e-fraud, monitor environmental changes, and measure organizations’ attitudes towards e-fraud threats.

The findings of the survey are interesting in understanding the attitudes of the South African and international business community to a significant type of electronic crime, namely computer fraud.

**Most respondents considered e-fraud to include:**

- Manipulation of data records held on a computer to disguise the true nature of a transaction (97%);  
- Hacking into an organization's computer system to steal or manipulate organizational information (97%);  
- manipulation of computer programs to disguise the true nature of a transaction (96%); and  
- Unauthorized transfer of funds electronically (94%).

Dumiak (2000) discusses the issue of security against credit card fraud on the internet, especially as e-commerce rises. The impact on advertising
campaigns used by companies to address consumers’ concerns for increased security is also discussed.

On September 23, 2003, the Identity Theft Resource Center released its survey of the impact of identity theft on 173 known victims. The survey findings were as follows.

- A large majority of respondents indicates the opening of a credit card (73%) or takeover of a card account (27%) to be among crimes committed.
- The emotional impact of identity theft has been found to parallel that of victims of violent crime.
- The responsiveness toward victims by the various entities with which they must interact continues to be lacking in sensitivity in most cases and has not improved.

In 2003, Federal Trade Commission (FTC) issued a survey on identity theft. The survey was conducted in March and April of 2003 with a random sample of over 4,000 households.

**Key findings include:**

27.3 million Americans have been victims of identity theft from 1998 to 2003. In 2003, 3.23 million consumers discovered that new accounts had been opened and other frauds such as renting an apartment or home, obtaining medical care or employment, had been committed in their name. 6.6 million Consumers experienced their existing accounts compromised by an identity theft. A total of almost 10 million individuals were victims of identity theft.

According to E-fraud Model (2003) presented by Pattama Malakedsuwana and Kenneth J. Stevens, the basic e-fraud model has been modified to accommodate both the technology advancement and nature of attack. Based on a broad definition of both e-crime and e-fraud, the resultant model describes the five key elements of e-fraud: perpetrator, mode of attack, target system, target entity and impact. It is envisaged that the model will allow the mechanics and context of e-fraud to be more fully understood, thus
assisting in the development and implementation of effective counter-measures.

On July 21, 2003, Gartner (www.gartner.com) released the results of a survey of 2,445 households regarding identity theft. The survey found the following:

- Identity theft is up nearly 80 percent.
- 7 million U.S. adults or 3.4 percent of U.S. consumers were identity theft victims in 2002.

On December 14, 2004, the Federal Deposit Insurance Corporation (FDIC) released a study on phishing and account-takeover including information about fraudulent automated clearing house (ACH) payments. The survey findings were:

- Consumers are attributing risk to their use of the Internet to conduct financial transactions, and many experts believe that electronic fraud, especially account hijacking, and will have the effect of slowing the growth of online banking and commerce.
- Up to 5 percent of the recipients of spoofed e-mails respond to them.
- An estimated 19 percent of “those attacked” have clicked on the link in a phishing e-mail. Most, if not all, large financial institutions and electronic bill-paying services (such as PayPal) have been hit with phishing attacks.
- Because many phishing attacks originate overseas and because the average life span of a phishing Web site is 2.25 days, the sites are hard to shut down.

Belcher (2004) addresses the rising problem of identity thieves targeting business records containing personal identification about employees. The author provides a number of suggestions for reducing the likelihood of workplace identity thefts and for protecting employees’ social security numbers.

According to MasterCard International investigation report data (2005) thieves breached the computer systems of credit-card processor of company
called Card Systems Solution from USA in 2005 and stole 40 million accounts affecting various credit-card brands. The breach has put consumer financial data at risk.

In April 2005, investment firm Amertrade announced that backup tapes containing details of nearly 200,000 account holders had been lost in transit.

Citigroup and Bank of America lost backup tapes with the data of nearly 3.9 million and 1.2 million account holders, respectively. And data-collection firm Choicepoint gave information on 150,000 U.S. citizens to criminal groups posing as legitimate businesses.

The Trojans virus that steals (2005) financial account information targeted only a handful of online banks. In August 2003, virus called PWSteal.Bancos.B stole account information from five banks. In February 2005, a Trojan named Trojan.Goldun.B [5] was discovered stealing account information for an online payment service called e-gold. The Trojan disguised itself as a security update for e-gold. When a user executed the deceptively-named file SecurityEgold.exe’, the Trojan registered itself as a browser helper object (BHO) and monitored Internet Explorer for visits to pre-defined URLs. Any account information that was gathered by the Trojan was posted via a PHP script on a domain controlled by the attacker.

Der Hovanesian, Mara (2005), focuses on cybercrime and suggests a little paranoia can protect consumers on the Internet. He discusses how Kathy Prati, a graphic designer in Sonoma Valley, became a victim of credit-card fraud; even with security software installed that could stop some hacker attacks and cannot stop all digital scams showing the weak link in the software.

According paper presented By François Paget (2007), McAfee® Avert® Labs, Financial fraud has many faces. Whether it involves swindling, debit or credit card fraud, real estate fraud, drug trafficking, identity theft, deceptive telemarketing, or money laundering, the goal of cyber criminals is to make as much money as possible within a short time and to do so inconspicuously.

The article by Simpson, Richard (May 2007), discusses fraud in the online retail industry. 64% of internet retailers have experienced fraud and that this costs those 5% of total annual revenues. An estimate of 1.5 billion
pounds in revenue is forecasted to be lost because cyber fraud by 2010. IMRG Projects and Marketing Director Andrew McClelland say that the development of Chip and Pin has contributed to the increase of online fraud. 3V technology presents a solution to online fraud however; there is a need to develop better security and checking protocol.

The article by Rohn (Aug 2007), Eli; Pinnero, Andrew, describes several techniques for detecting computer crimes and information security breaches. According to annual surveys published by the U.S. Federal Bureau of Investigation's (FBI) Computer Intrusion Squad and the Computer Security Institute (CSI), the financial impact of computer crime and information security breaches has declined since 2001. On the other hand, the 2006 study revealed that security awareness and implementation of proactive countermeasures have continuously reduced the number of cases.

The article by Latto, Aaron (Sep 2008), presents a discussion of data breaches and how these occurrences are best managed. It suggests that insurance adjusters, claim managers, and risk experts need to be well-versed with best practices relating to the problem of cyber fraud. With modern day technology, gathering large amounts of private information has become easy and with it the risk of theft, loss, and exposure has increased. Data breaches can also lead to identity theft and fraud.

According to Whitepaper published (2009) by VeriSign in 2009 on fraud alert, reported that unique phishing attacks submitted to APWG rose 13 percent during the second quarter of 2008 to more than 28,000. It also reported that, during the same period, the number of malware-spreading URLs infecting PCs with password-stealing code rose to a new record of more than 9,500 sites, a 258% increase compared with the same quarter in 2007.

According to Symantec (2009), malicious activity in 2008 amounted to 60 percent of all the activity they have recorded since they started keeping records. In 2007, they recorded 1.6 million new malicious code signatures and blocked 245 million malware attacks from their users every month.

Many of these attacks when the words malware or malicious codes are used are designed to steal information (preferably financial) or take command and control of a computer. Once command and control of a computer is accomplished it’s called a zombie and networked into a botnet. A botnet
works as a super computer and is used to spam the electronic universe. Some of these spam e-mails contain even more malware, which infects more unprotected systems.

The article in Managing Accounts Payable journal issue (2009), provides information on the practices that could prevent electronic payment fraud in the U.S. These include the utilization of the fraud defenses offered by the bank to protect accounts from unauthorized Automated Clearing House (ACH) debits. The other one is to encrypt the transmission of banking information from ACH transactions using a commercially reasonable security technology. The final step is the setting up of alerts to notify the managers of payments.

One of the studies on the underground economy of stolen or compromised sensitive information (2009) was done by Jason Franklin, Vern Paxson, Adrian Perrig and Stefan Savage. In this study, using 7 month trace of logs of underground market collected on public internet chat networks, different types of frauds like credit card theft, identity theft, phishing and online credential theft were categorized. Also discussed the nature and causes of the wealth of Internet miscreants.

One graph from this paper shows the most common types of data that were advertised as being for sale by cyber-criminals. The graph is shown as below.

![Figure 2.1: Stolen Data Vs Sensitive Data type](image-url)
This graph shows that credit card information is widely available. It's more available than Social Security numbers or ATM PINs. This means that it's probably the case that credit card information needs to be protected much more than it's being protected.

The article by Wolfe (2009), Daniel, reports that hackers are focusing more attention on the bank accounts of businesses than on those of individual consumers due to their tendency to keep larger balances and have less regulatory protection.

The article by Hill (2009), Kashmir, discusses the involvement of forensic accountants in criminal and civil litigation in the U.S. It refers to the case of Allen Stanford for defrauding investors who purchased about seven billion dollars for certificates of deposit which is administered by Stanford International Bank. According to Ronald L. Durkin of Durkin Forensic, the biggest challenge in forensic accounting is gathering records which include millions of computer files and electronic documents.

This paper by Devos, Jan; Pipan, Igor (Dec 2009), is intended to provide accumulative and organized information of the efforts made to protect businesses from fraud. The authors try to reveal the effectiveness and efficiency of the current fraud combating techniques and show that organized worldwide efforts are needed to take care of the larger part of the problem.

To gain insight into the costs and benefits associated with internal control protocols, Tibbs, Samuel L examines the market response to allegations that firms have engaged in financial fraud, bank and wire fraud, billing fraud, embezzlement, bribery and kickback schemes. These allegations are investigated as they represent cases most closely related to the treasurer's mandate of financial controls, payment execution and oversight of cash. The study finds that, on average, allegations of misconduct result in statistically significant losses in firm value and increases in total risk. The results are found to be sensitive to the type of misconduct investigated.

The article reports on Heartland Payment Systems Inc.'s claim that payment card data from customers at several restaurants in the U.S. may have been robbed. It notes how they detected data-stealing software imbedded by criminals known as "global cyber-fraud ring" within its network. It also discusses the means by which the thieves operate. Moreover, Heartland
presents Information on the data, systems and operations unaffected by the breach.

The paper by Khanna, Ashu; Arora, Bindu, examines the issue of frauds from the perspective of banking industry. The study seeks to evaluate the various causes that are responsible for banks frauds. It aims to examine the extent to which bank employees follow the various fraud prevention measures including the ones prescribed by Reserve Bank of India. It aims to give an insight on the perception of bank employees towards preventive mechanism and their awareness towards various frauds. The study signifies the importance of training in prevention of bank frauds. A strong system of internal control and good employment practices prevent frauds and mitigate losses.

In this report\textsuperscript{23}, (2010) how criminal hackers used technology from 1960-2009, to breach data security can be seen. Criminal hackers manipulated the new digital phone systems in the 1960s and 1970s; then they moved on to using modems and hacking into mainframes in the 1970s and 1980s; then they exploited the local area network technology(LAN) and the Internet in the 1980s. Malware writers moved from boot-sector viruses on floppy disks in the 1980s to file-infector viruses and then to macro viruses in the 1990s and now vigorously exploited worms and Trojans for botnets to steal sensitive information from the Internet.

\textbf{2.4 Literature survey of Credit card}

Matthews and Slocum (1969) investigate the correlation between social class and credit card purchasing behavior. Results illustrate a significant relationship between credit card usage and consumer social class.

Garcia (1990) explores the history of credit card growth in this article. An assessment of selected previous research is given and an economic model of a rationed market is presented. Next, the author explores the effects credit cards have on social and economic variables, particularly consumption and the demand for money. Finally, credit cards’ role in the electronic money era is assessed, especially relating to issues of security and privacy.
Lenora (1991) focuses on using behavior to segment credit cardholders into four categories. Each segment is characterized according to several factors, such as the manner in which the balance is paid each month and the amount of monthly activity.

Cole (1998) gives a detailed bottom-up academic explanation of how the whole consumer credit process works from the overall economy to the actual credit approval process at a bank. The study provides very thorough and detailed reference on the whole system and infrastructure depends on the perceived value of information and the amount of it, which is purchased.

Medintz (1998) focuses on credit monitoring services in this article and gives both advantages and disadvantages of such. The author finds that few credit protection services are worth the cost, stating that the risk of private information being stolen on the internet is often overblown and consequences are not as severe as the credit monitoring agencies would lead consumers to believe.

Stanford (1999) provides a great portrayal of the marketing manoeuvres of various credit card companies and their endeavours to reach untapped markets it provides solid metrics on the average number of credit cards and debt upon graduation.

Aquino (2002) advocates that consumers should educate themselves before applying for a credit card and gives recommendations on how to use credit cards responsibly. Topics discussed include deciding how credit balances will be paid, number of cards to own, and how to calculate the average daily balance.

Hogarth (2002) explains consumer complaint resolution and the elasticity of the credit card market. Some pertinent information on the business dynamics of the credit card industry is provided.

Brooker (2004) examines the creation of the credit card and how it has revolutionized American business. The author points out the impact credit cards have had on modern day businesses, such as FedEx, Wal-Mart, and eBay. The author also chronicles the environment in which purchases were made in past and considers how modern-day business would be if still cash-based.
2.5 Literature survey of e-banking

Desai, Subhash. Siliconindia (Aug 2001), has discussed the technology requirements of the electronic banking sector of India. Improvement in the information technology infrastructure of the banking industry to global standards; greater connectivity in the gateways for electronic bank payments.

The paper on “E-banking- modern banking services” by Miranda-Petronella, Vlad (2009). Annals, has discussed the payment, computational application, an authentication method and a communicational average.

The study conducted by Hung, Humphry; Wong, Y. H(2009) is to develop and validate a model to analyze the inter-relationship between information transparency and the protection of digital privacy of customers, from the perspective of e-services providers.


The interpretive case study conducted by Merisalo-Rantanen, Hilkka; Rossi, Matti; Hallikainen, Petri; Nurmimäki, Kari, (2009) examine the processes and the related information systems (IS) fostering user influence in a large scale e-banking case and focuses on user involvement in the IS evolution.

The paper by Sharma, Dhiraj (Mar 2009) in “ICFAI Journal of Management Research” discusses and highlights the prospects and perils associated with the banking technology in India. It attempts to investigate, using document analysis (Neuman, 1997), the problems and prospects of banking-technology interface in India.

The paper presented by Nandan, Geetika; Nandan, Tanuj; Upadhyay, Ashwani K. R, (May 2008) discusses the concept of internet banking, perception of internet bank customers, non-customers and issues of major concern in internet banking. The findings of the survey provide valuable insights into concern for security, reasons for lower penetration, and likeliness of adoption, which have been used to make useful recommendations.
Eric Robbins paper in RMA journal (2010) discusses research on electronic banking (e-banking) services and explains how the adoption of these services varies among several demographic groups. He explores the attitude of consumers toward e-banking technologies and its relationship with different demographic characteristics in the development of strategically e-banking platforms. Several findings of the study are mentioned including the use of conventional banking products such as direct deposit, debit cards and automated teller machines (ATM).

Mr. Holmquist, Eric. In RMA Journal (2010) focuses on principles of risk management that should be followed by banks for the implementation or expansion of electronic banking (e-banking) products and services. He suggests that banks should start with risk assessment in several disciplines including security, information technology and customer service. Other considerations include governance starting with the clear knowledge of the board of directors about products and services.

The results of this study conducted by Mahdi Salehi; Alipour, Mehrdad (Feb 2010) shows that e-banking serves several advantages to Iranian banking sector, however, the study also shows that the Iranian customers have not enough knowledge regarding e-banking which is rendered by banking sector in Iran.

The paper submitted by Uppal, R. K., IUP Journal of Bank Management, (Feb 2010) examines the productivity and profitability in pre- and post- e-banking periods and highlights the emerging issues and new strategies to enhance the performance of bank groups in today's liberalized, globalized and IT era. The paper concludes that though there is a paradigm shift in the performance of all bank groups in the post e-banking period, new private sector banks and foreign banks have an edge over Public Sector Banks (PSBs). The fully IT-oriented banks have become both a threat and a motivation for the PSBs. The paper stresses on customer-centric, proficiency in managing assets, technology, skilled staff, transparency, human resource management policies, customer relationship management, and merger and acquisition policies as vital factors to enhance the performance of banks to face the emerging global competition.
2.6 Literature survey of e-payment

This article by Newman, Simon; Sutter, Gavin, (Jul. 2002) in three parts examines the legal issues raised by the development of the smart card. It explores contractual, liability at intellectual property rights issues and assesses whether a suitable legal framework exists in which smart card use can flourish and grow.

Sheng-Uei Guan; Feng Hua (Sep. 2003) propose a multi-agent mediated electronic payment architecture in this paper. It is aimed at providing an agent-based approach to accommodate multiple e-payment schemes. Through a layered design of the payment structure and a well-defined uniform payment interface, the architecture shows good scalability. When a new e-payment scheme or implementation is available, it can be plugged into the framework easily.

The article by Flanigan, Paul D, (Dec. 2005) reports on the findings of a research into consumers' online payment preferences in the United States. The electronic payments and expedited payments, commonly known as convenience payments, are gaining in popularity. The reason U.S. consumers have turned to expedited payments, however, has more to do with their hectic lifestyles than financial issues. The implications are broad and the information critical and timely as billers turn to electronic payment processing solutions to enhance cash flow while improving their billing, payment and remittance processes.

In this article Sanayei, Ali; Rabbani, Hamed, (Feb. 2006) has discussed the e-banking evolution and explain the emerging of e-banking services, E-payment system as well as legal, risk management challenges, and have presented necessary suggestions for managing e-banking.

In 2006, SMS services provider TynTec announced the launch of mobile One-Time Passwords (OTP) for the banking industry.

The paper by Wonglimpiyarat, Jarunee, (Dec. 2007) is concerned with the business strategy in managing payment innovations. Particularly, the study looks at the smart card - electronic cash (e-cash) innovation in the financial service industry. The smart card e-cash has yet to overcome obstacles to its diffusion. Given the e-commerce opportunity, banks and non-
banks compete to deploy smart card technology for internet use. A review of previous payment innovations is also carried out to provide suggesting direction on the innovation proliferation.

The article by Cotteleer, Mark J.; Cotteleer, Christopher A.; Prochnow, Andrew, (Jun. 2007) discusses the future of corporate payments and how businesses plan to address the challenges of integration, security, and remittance standards.

Keeping in view, the serious threats of phishing (Aug. 2007) attacks analyzed by Singh, N. P, and the trends of major activities of the phishing across globe specifically in the banking sector. In addition, author analyzed the reasons for increase in phishing activities, types of phishing techniques, and process of phishing.

The article by Bland, Vikki, (Dec. 2008) focuses on the benefits and risks of electronic payments. Statistics NZ revealed that the value of total electronic card transaction (ECT) series had increased 0.8% at a value of $4.5 billion in September 2008 compared to August 2008.

The paper by Flatraaker, Dag-Inge, (Jan. 2009) describes how some banks and banking communities in the last two decades, especially in the Nordic area, have been able to take advantage of technology and new payments channels to re-engineer their payments business, and how they interact with their customers. This paper also gives some insight into how the Single Euro Payments Area and other standards initiatives could potentially enable those banks and banking communities lagging behind to bridge the gap, as well as how internet and mobile banking will influence the payments landscape and create opportunities for re-engineering in the future.

The article in Managing Accounts Payable, (May. 2009) reports on the findings of the Association for Financial Professionals (AFP) Electronic Payments Survey in the U.S. The survey reveals that 74 percent of the typical company's business-to-business (B2B) payments are made through checks in 2007. Some of the barriers to increased use of electronic payments include the shortage of information technology (IT) resources and lack of standard format for remittance information.
2.7 Literature Survey of Information Security

In ABA Banking Journal issue (Nov. 2004) a dialogue with Symantec Corp. executive David Moulton on bank information security as it relates to compliance.

The article by Bruce Jay; Huszar, W. Alison, (Aug. 2005) provides information on banks' information security programs that are useful for consumers.

The article by Sausner, Rebecca, (Nov. 2006) information on a new firewall desktop used by the Community Bank for online security. According to the bank's information security officer Aaron Friot, the system offers intrusion prevention without the constant sitting of the employees, and is user-interactive. The intrusion protection product is called "Blink," and is developed by eEye Digital Security. The system has an inbuilt systems firewall, and a malware engine for detecting spyware.

2.8 Literature survey of Security standards

Sathye (1997) reviewed the status of internet banking in Australia. The study found that only two of the 52 banks started internet banking services. He opined that education would be a crucial factor for expanding internet banking in Australia. If customers are convinced about the various advantages of internet banking they will start asking for this service from their banks, and will put pressure on the banks to go ahead with internet banking.

- Filotto et al. (1997) illustrated that the adoption rates of ATM were higher among young users. In addition,
- Barnett (1998) findings proved that younger consumers are more comfortable in using e-banking.
- Katz and Aspden (1997) findings explained that males were more likely to adopt e-banking than females.
- Mookerji (1998) explored that internet banking is fast becoming popular in India. Nevertheless, it is still in its evolutionary stage. They expect that a large sophisticated and highly competitive internet banking market will develop in future.
Joseph et al. (1999) examined the influence of internet on the delivery of banking services. They found six primary dimensions of e-banking service quality such as convenience and accuracy, feedback and complaint management, efficiency, queue management, accessibility and customization.

Mols (1999) acknowledged that the internet banking is an innovative distribution channel that offers less waiting time and a higher spatial convenience than traditional branch banking with significantly lower cost structure than traditional delivery channels. Internet banking reduces not only operational cost to the bank but also leads to higher levels of customer satisfaction and retention. As a result internet banking is very attractive to banks and consumers, who now have higher acceptance to new technology (Polatoglu and Ekin, 2001, Mols, 2000, Sathye, 1999, Wisner and Corney, 2001).

This article by Wool, Avishai, (2002) discusses the failure of security standards in computer systems. Working on a standard has its own set of challenges. A standards body involves many parties with conflicting agendas, many of them powerful corporations. Furthermore, a standard is not measured by excellence or novelty: It should be a working design that is an acceptable compromise between the interests of all the parties involved. In short, a standards body is not an environment that encourages scientific discourse.

The paper by Backhouse, James; Hsu, Carol W.; Silva, Leiser, (Aug. 2006) addresses the role of power and politics in setting standards. It examines the interaction of external contingencies, powerful agents, resources, meaning, and membership of relevant social and institutional groupings in generating successful political outcomes. To study these interactions, the paper adopts the circuits of power, a theoretical framework taken from the social sciences, and applies it to understanding the creation and development of the first standard in information security management. An informal group of UK security chiefs sparked off a process which led first to BS7799, the British standard, and later to ISO 17799, the international standard.
This article by Owen, Michael; Dixon, Colin, (2007) discusses the Payment Card Industry Data Security Standard, also known as the PCI DSS. This standard has been assembled by the PCI group as a security baseline for all processors, handlers, or collectors of cardholder data bearing the mark of any of the members of the PCI.

The article by Garry, Michael, (2007) reports on the move of credit card industry in the U.S. to take some rigid steps that can help retailers improve security of their data cards. According to the article, through the sector's Payment Card Industry (PCI), the group is giving retailers greater predictability to their audits. In addition, it states that several states have already started enacting the in-transit data encryption system.

This article by Garry, Michael, (2007) reports that retailers are having difficulties in complying with the payment card industry data security standard (PCI DSS), according to Dave Hogan, National Retail Federation's senior vice president and chief information officer. Visa USA imposes fines for non-compliance on a retailer's bank, which can pass them on to the retailer. Hogan remarked that one of the primary challenges for retailers was receiving timely feedback from the card associations on whether they are in compliance with the standard.

The article by Reedy, Dennis; Conway, Walt, (2007) discusses strategies for Payment Card Industry Data Security Standard (PCI DSS) compliance. The authors suggest gathering information to make a business case and deciding how to communicate the message to department and division managers. A working team must be assigned that includes both finance/treasury and security expertise at a minimum. It is noted that achieving PCI compliance is a continuing process which does not end with being certified as compliant.

The author Garcia, Andrew (2008) reflects on the changes to Payment Card Industry (PCI) Security Standard in the U.S. He expects further enhancement to the wireless recommendations that will serve to adequately protect data and networks. He asserts that the new draft will not go so far as to require the use of enterprise-grade and certificate-based encryption schemes. He suggests that the standard would have the added benefit of
switching wireless analysis from a capital expense to an affordable operational expense.

The article by Garry, Michael, (2008) reports that a payment card industry group, the PCI Security Standards Council LLC, has launched a program to bring greater consistency to the auditing process for retailers so that they adhere to a credit and debit card data security standard. The Council has developed a quality assurance program for the various companies, known as qualified security assessors, to inspect retailers' store systems and networks for compliance to the Industry Data Security Standard.

The article by Collins, Anne, (2008) focuses on the new data security standards introduced by Payment Card Industry (PCI), compliance standards for organizations receiving revenue from credit cards to protect them from the theft of credit card information. PCI standard is governed by the Payment Card Industry Council and overseen by the PCI Working Group. Other benefits and advantages of becoming compliant are presented.

The article in Convenience Store Decisions, (2008) offers information on the participation of the National Association of Convenience Stores (NACS) in the Payment Card Industry (PCI) Security Standards Council in the U.S. The organization officially joined more than 20 other members which are committed to evolve the PCI Data Security Standard (DSS) and other payment card protection standards.

The article by Mehta, Kamlesh, (2008) reports on the new Version 1.2 Data Security Standards (DSS) released by the Payment Card Industry (PCI) Council, which will offer improved flexibility to address security challenges. It relates that the DSS impact all types of enterprises and can create risk beyond retail operations. Moreover, it contends that automating the process of tracking all information technology (IT) changes and configuration helps future proof processes against new revisions to existing PCI requirements.

The article reports by Twentyman, Jessica, (2008) on the problems encountered by online businesses regarding protection of their customers' data from hackers. One example is that of British clothing retailer Cotton Traders, which admitted in June 2008 that hackers had gained access to the details of the credits cards used by their website customers.
An article by Pickles, Chris, (2008) the financial services industry has a long journey ahead of it as it migrate to the use of the ISO 20022 standard. Cross-border securities settlement processes have moved to the use of ISO 15022 and most domestic securities settlement is still carried out with relatively little use of the standard. Meanwhile, more and more of the industry's pre-trade and trade activities have moved to adopt the Financial Information exchange (FIX) protocol standard, as have exchanges and other core infrastructures. The process of migration is further complicated by the broad range of changes that are continually taking place across the industry, making it impossible to find a 'quiet time' during which changes could be made with minimal disruption to a firm's usual business. Adding to this difficulty is the fact that industry standards are being further developed even while market participants are implementing current versions. Having the right tools in place to plan for and complete such a journey is vital to success.

The article in Venulex Legal Summaries, (2008) discusses several accepted data security standards that will protect a company from liability or government enforcement when a data breach occurs. The ISO 27000 series of standards are considered by many as the data security gold standard because they establish specific guidelines for instigating and enhancing information security management within an organization. Another standard is the Payment Card Industry or PCI standard.

This article by Morse, Edward A.; Raval, Vasant, (2008) examines the varying and sometimes complementary roles that legal obligations and private ordering play in incentivizing security measures to protect consumers. Also this article evaluates the basic framework of PCI DSS and raises issues for further development as the government, the legal system, and the industry cope with security threats in this environment.

The article by Jackman, Michael, (2008) presents information on the security standards for payment card industry in the U.S. It is stated that all businesses that handle between 1 million and 6 million credit card transactions a year were supposed to adopt the payment card industry's new data security standard (PCIDSS) by December 31, 2007. It highlights the case of security breach at TJX companies. Lawsuits seeking damages on behalf of customers and banks are pending in federal or state courts in three cases.
The company was charged for failing to comply with the PCI standards for data and computer security.

In this article by Iacono, Luigi Lo; Wang, Jun, (2008) discusses the web service (WS) related security standards that provide a comprehensive framework to develop and implement security systems for WS environments. These standards are often broad in scope, and the price of this generality is a high level of complexity. This in turn can lead to potential security problems. Web services are a powerful set of technologies that can be used to build service-oriented architectures (SOA).

The article by Oehlsen, Nadia, (2008) reports that the major changes to the newest version of the Payment Card Industry Data Security Standard have become good news for industry to develop security standards in France. A number of merchants are withholding data about possible network insecurities from the organizations they hire to improve their PCI compliance. Despite some private confessions of security imperfections, beyond disagreement is the need for every entity that touches payment card data to keep it safe.

The article by Cameron, Derrick, (2008) reports on the release of a document entitled "PCI Data Security Standards" by the Payment Card Industry (PCI) Security Standards Council in Great Britain. It states that the council was formed by the leading payment brands, including Visa and Mastercard to develop data security standards in response to rising fraud within the industry. The standards were designed to ensure organizations adopt consistent security measures to proactively protect customer account data.

This article by Braun, Robert E, (2008) explains that new U.S. regulations for credit card security and data protection could make retailers liable in cases of a data breach. It advises retailers to adopt the Payment Card Industry Data Security Standard (PCI-DSS) as this will have a significant impact on the liability of merchants who use credit card transactions. The impact of PCI DSS is not only to achieve greater protection for customer data, but has become a de facto standard of care which can result in unforeseen liability for a merchant whose data is compromised.
The article by Fluss, Donna, (2008) discusses compliance with the Payment Card Industry (PCI) security standards. In 2007, PCI standards have become a requirement for a lot of contact centers. Though the PCI Security Standards Council sets the standards, it is actually the card companies that enforce compliance and impose penalties to those who are not compliant. Generally, U.S. merchants that do not comply with the PCI data security requirements might face class action suits and other financial or operational consequences.

The article by Sullivan, Richard, (2008) presents a discussion on the potentiality of smart cards to provide strong payments authorization in response to the problems of payments fraud and theft identity in the U.S. It provides a review of the costs of payments fraud and describes how payments fraud is related to identity theft. It explains how smart cards work and how they can improve payment authorization and provides further description of the weaknesses that can remain even with the use of smart cards. Moreover, it discusses the incentive for adopting payments smart cards and for upgrading payments security standards and examines the market processes that determine the security standards used in payment smart cards.

In this article, Updegrove (June 2009), Andrew survey the challenges we face to implementing effective cyber security, the types of standards used to provide it, the organizations that develop such standards, and the initial steps that the United States federal government is taking to implement them.

The article published in Communications of the ACM, discusses information security management standards, which focus on the existence of process and not the content of what it is securing. Information security management standards like BS7799 are widely used and advocated by researchers and practitioners; they have a limitation in that they focus on ensuring that security processes exist while being unconcerned about how these security processes can be accomplished in practice. The article examines how this problem pertains to four different information security management standards.

The article by Howard, (2009) discusses the concerns of convenience store operators regarding the Payment Card Data Security Standard
compliance. They need to find out whether their POS system supplier's application has been developed to meet the standard. If their point-of-sale systems fail to meet the standard, they should upgrade their software and hardware. Other operators find it hard to meet the deadline as they have difficulty to get enough technicians to get such things upgraded.

An interview with Bob Russo (2009) of PCI Security Standards Council (SSC) is presented. He explains how the PCI SSC started its operation as an open global forum for the development and implementation of account data security standards. He discusses particular challenges linked with maintaining payment card security and the roles of other players in the payment card chain in terms of keeping security. When asked what are the greatest security threats he sees in the future, Russo mentions complacency.

The article in Lodging Hospitality journal, (2009) offers information on the version 1.2 of the PCI Data Security Standards (PCI DSS) released by the PCI Security Standards Council. Feedback on how lodging and hospitality organizations deploy security requirements is included in the update and more than 2500 queries and suggestions were considered. The Version 1.2 provides consistent use of terms and greater flexibility such as decreasing mandatory review of firewalls from a minimum of every three months to every six months and the sunset date for the use of Wired Equivalent Privacy is one of the significant change.

The article by Determann, Lothar; Hwang, Jesse D, (2009) discusses various data privacy and security laws in government agencies and companies in the U.S. It cites the Health Insurance Portability and Accountability Act (HIPAA) which apply to health care companies and the Gramm-Leach-Bliley Financial Services Modernization Act for financial services providers. It highlights the requirements for industry group to implement data security standards, and sanctions for companies which will not comply.

The article by Boyer, Meghan, (2009) reports on the difficulty faced by some merchants in complying with the Payment Card Industry (PCI) data security standard in the U.S. It notes that smaller retailers are struggling to bond with security standards. It points that merchants should keep up with the
challenging standards, despite their size. They may also comply by installing software patches and by examining holes in their networks.

The article by Morrison, David, (2009) reports on the examination of the data security standards of the credit card industry in the U.S. Congress. The examination concluded that if the credit card industry cannot address its own fraud risks, the Congress might step in with federal legislation. The Congress also suggests that the industry must have a better encryption of data, more frequent updates on criminal tactics and must have new technologies to prevent identity theft.

The article by Frumkin, Paul, (2009) reports that the 14th annual International Foodservice Technology Exposition (FS/TEC) held in Orlando, Florida, during February 2009 provided details related to the revised Payment Card Industry (PCI) Data Security Standards (DSS). According to experts at the event, it will be impossible to achieve full compliance of PCI DSS Version 1.2, and operators will have difficulty in completely protecting credit and debit card information.

According to report by Technology company NCR Corporation (NYSE:NCR), (2009) version 5.4 of its Advanced Store point-of-sale (POS) solution has been confirmed as meeting the most current standards designed to protect consumers’ credit card information from potential security breaches.

An interview with Visa Inc. security executive Ellen Richey in 2009 in the U.S. is presented. She states that the cyber security post proposed by President Obama is positive news; it is based on the national cyber security initiative. She believes that the death of the Payment Card Industry data-security standards is dangerous, because it will misinform consumers that it is useless to apply the standards. She cites that there should be coherence in the application of basic technology worldwide.


The article appeared in CardLine Journal, (2009) reports on the deadline set by Visa Inc. to global acquirers to ensure that all merchants use
software applications that comply with the Payment Card Industry Payment Application Data Security Standard. It states that the standard helps ensure that software capable of receiving electronic payments does not store sensitive transaction data. It notes that acquirers have until July 12, 2012 ensured existing merchants use compliant software.

The article in NZ Business, calls for businesses that perform or process credit card transactions to comply with the Payment Card Data Security Standard (PCI DSS). It stresses the need for businesses to implement file integrity monitoring controls on the technology that support these transactions. It also suggests businesses to utilize systems and tools that make PCI DSS compliance easy to maintain such as configuration assessment and change auditing tools.

The article by Amato-McCoy, Deena M, (2009) discusses the 1.2 Payment Card Industry Data Security Standards in the U.S. The new standard requires few recommendations and investments for those up to date with compliance. The 1.2 standard requires the use of antivirus software for all operating system types, including point-of-sale systems. Overall, the new standard clarifies requirements within wireless security, new anti-virus protection and network firewall settings.

The article by Aguilar, Melissa Klein, (2009) presents a report from the Institute of Internal Auditors regarding companies' compliance with the Payment Card Industry Data Security Standard (PCI DSS). It states that only 56% of companies comply with PCI DSS. It offers several suggestions for more efficient compliance process including educating of staff and internal auditing to secure data from risks. It also suggests relating organizational and industry practices to determine possible security failures.

The article by Bartlett, Neil, (2009) announces the creation of Payment Card Industry (PCI) Security Standards Council, which aims to develop, maintain, and distribute the PCI Data Security Standards. The council is a global forum on security standards for account data protection which is headed by Seana Pitt, vice president of American Express. Moreover, the council plans to enhance the data security standards to include new requirements that mitigate emerging payment security risks.
The article in CardLine, (2009) reports that six merchant trade groups including the U.S. National Retail Federation and the National Restaurant Association have submitted a joint letter to the U.S. Payment Card Industry (PCI) Security Standards Council calling for changes to the PCI data-security standards. In the letter the coalition has urged that council members be allowed to formally review and comment on revisions to the standards before the full council approves them.

The article by Rapport, Marc, (2009) presents the results of Aite Group LLC’s report "Card Data Security: In Search of a Technology Solution" in the U.S. It shows that there is no vaccine against card data security breaches in the country. It was found out that the prognosis for the continuing ailment indicates that there is no fast cure. It points out that fixing card security will cost an estimated 100 billion dollars. It suggests that changes in Payment Card Industry Data Security Standards (PCIDSS) are needed.

The article in CardLine (2009) implies that the banking industry's fundamental standard for protecting payment card data may not be enough to fight fraud. This was reported by "American Banker", a CardLine sister publication. It is stated that the major card networks long have urged merchants to adopt the Payment Card Industry Data Security Standard, but now that most big retailers are in compliance, observers are beginning to shift their views on what is needed to thwart fraudsters.

The article by Birch, Ray, (2009) reports on the need for tighter Payment Card Industry (PCI) Data Security Standards which arise after an announced data breach at Heartland Payment Systems LLC in Princeton, New Jersey. The company indicated that malicious software compromised data crossed its network and that stolen data include names, numbers and card numbers. CUNA Mutual recommends several actions that the PCI has to consider to determine high risk exposure for future fraud.

The article by Chickowski, Ericka, (2009) reports on the wireless security guidance offered by the PCI Security Standards Council (SSC) which will provide greater clarity in applying to wireless technology securely within payment card transaction environments. The guideline is believed to be a welcome relief to some who complained that the main body of the security standard is too ambiguous. Bob Russo, PCI SSC general manager, says the
standards aim to create a more impressive payment card security environment.

The article by Child, Mark. Caterer & Hotelkeeper (2009) presents suggestions on how to comply with the latest Payment Card Industry (PCI) security standard in Great Britain. The author says that the new standard will affect all those business owners who accept credit or debit card payments. According to him, they should be aware of their obligations under the data security standard as failure to comply with the standard may result in severe business losses. He also suggests reviewing security arrangements regularly.

In this article by Rutherford, Bruce, (2009) the author discusses the Payment Card Industry's (PCI) full year of releases and meetings as PCI's next iteration takes shape. As chair of the PCI Security Standards Council, Bruce Rutherford emphasizes its role in the promotion and development of several standards to protect account data in payment transactions. An overview of what to expect for 2010 is also presented.

The article by Villiers, Meiring, (Jan. 2010) explores the legal standard of information security within the aspects of law, economics and technology, and its implementation in an information security environment. It discusses the principles of computer viruses and worms, and the common virus detection technologies. It offers several examples which would show the cost benefit of an untaken precaution.


The Article by Schell, Ernie, (2010) discusses the security of direct commerce order management systems. It cites that such systems should comply with the data security standards that were developed by the Payment Card Industry Security Standards Council (PCI SSC) by July 1, 2010. The standards are included in the Payment Application Data Security Standard (PA-DSS), which is applicable to all order management systems and to e-
commerce shopping carts that are external and not interfaced with e-commerce platform.

In this research paper by EL Yamany, Hany F.; Capretz, Miriam A.M.; Allison, David S, (2010) they propose an intelligent SOA security framework by introducing its two most promising services: the Authentication and Security Service (ASS), and the Authorization Service (AS). The suggested autonomic and reusable services are constructed as an extension of WS-security standards, with the addition of intelligent mining techniques, in order to improve performance and effectiveness.

The article by Clutterbuck, Peter, (2010) offers information on the significance of the Payment Card Industry Data Security Standard (PCI-DSS) for businesses in Australia which handle the transmission of card data. It says that the PCI-DSS is a standard protecting the data of the debit and credit cardholder whenever that data are being processed, transmitted and stored. It also notes that the PCI-DSS structure focuses on 12 basic security requirements wherein non-compliance penalties are set by an individual card brand.

The article by Chickowski!, Ericka , (2010) focuses on the measures to be kept in mind for Information Technology (IT) organizations regarding the payment card industry (PCI) data security standard (DSS). Configuration and change management are critical to reduce the vulnerabilities in the IT infrastructure. Data discovery and classification is another tool which provides room for growth for the PCIs. Web monitoring and filtering may help in preventing unauthorized access to endpoints through web site infections.

The article by Klie, Leonard, (2010) reports that a 2009 research by call recording software provider Veritape found that most of the call centers in Great Britain violated the Payment Card Industry Data Security Standard (PCI DSS). They did not delete or mask credit card details in their call recordings, which put 285 million card transactions at risk, according to the research. PCI DSS is a security standard for the protection of customer account data. It prohibits the inclusion of card numbers and security codes in telephone recordings, among other security measures.

The article in CardLine journal, (2010) reports on an announcement by Global Collect regarding it joining the PCI Security Standards Council as a
participating organization to develop the data protection standards. All the major card brands including MasterCard Inc., Visa Inc., and American Express Co. are being endorsed by the PCI Security Standards Council. Processing services for international Customer Not-Present (CNP) channels are being provided by Global Collect.

The article (2010) reports that according to the latest compliance update from Visa Inc. for the quarter ended December 31, 2009, 96% of Level 1 merchants with 6 million or more annual Visa transactions were compliant with the Payment Card Industry (PCI) Data Security Standard in comparison to 97% in the last quarter. It says that compliance rate for Level 2 merchants was 94% and for Level 3 e-commerce merchants, the rate was described as moderate.

The article by Boyer, Meghan, (2010) reports on the need for independent sales organizations (ISOs) to educate themselves on aspects of data security and compliance in the payments industry to serve their clients better in the U.S. A study on Payment Card Industry Data Security Standard compliance found that only 2% of large businesses fail in compliance audits, while 98% pass. The study was conducted by Traverse City, Michigan-based research group The Ponemon Institute LLC to 155 qualified security assessors.