**International Journal of Commerce and Management Research**
**ISSN: 2455-1627**
**Impact Factor: RJIF 5.22**
**www.managejournal.com**
**Volume 4; Issue 1; January 2018; Page No. 62-66**

# Electronic payment: A boon or bane

**[1] Dr. P Sankarappa, [2] Dr. NK Pradeep Kumar**
[1] PDF (ICSSR), Dept. of Commerce, S.V.U College of CM & CS, S.V. University, Tirupati, Andhra Pradesh, India
[2] Academic Consultant, Dept. of Commerce, S.V.U College of CM & CS, S.V. University, Tirupati, Andhra Pradesh, India

**Abstract**
The rapid growth of the Internet over the past several years has been fueled mainly by the sharing and transferring of vast amounts of information. This comes from the increased use of the Internet for commercial business transactions, which gives birth to electronic fraud (e-fraud) problems. Payment fraud is one of the most significant problems a self-storage operator faces. Most business transactions are concerned with three types of security. First, they wish to ensure the positive identity of the customer, and that all transactions are sent to the right customer. Second, they want to protect sensitive customer information, such as credit card numbers, bank account numbers, or other personal and financial data. And third, they want to make sure that the data is not altered or changed as it is transmitted across the Internet. This study seeks to redress this situation through the development of a model of the process of e-fraud, using the existing literature as a guide. Based on a broad definition of both e-crime and e-fraud, the resultant model describes the key elements of e-fraud and recommended six-step protocol to reduce merchant-service fraud. It is visualized that the model will allow the mechanics and perspective of e-fraud to be understood precisely, thus assisting in the development and implementation of effective safety measures.

**Keywords:** electronic fraud, electronic business, electronic crime, fraud

## Introduction
Electronic payment system is a modern way of monetary transactions, which bear its roots and strength from the current explosion in information and computer technology under the support of Network technologies. The electronic payment transactions have been in use for several years, even the automatic teller machines (ATM), credit card, debit card, direct deposit and direct payment etc. However, these methods took some time for consumers to become familiar with them and trust worthy enough for use. The methods no doubt provided for fast, easy, paperless transactions, which have cost benefits and savings. One particular feature of the above methods is that consumers have been using them offline. That is, not on a personal computer or on the Internet. The banking industry and software companies have been working together to develop effective on-line payment system that would be acceptable to the merchants, consumers and as well safe guard the banking sector.

## Objective of the paper
The present paper aims at focusing forms and model of e-payment frauds and prevention measures to reduce the fraud.

## On-line payment systems
The characteristic features of on-line payment systems include:

- Transaction Type: This has to do with the type of transaction the system supports. That is to say, whether system supports transactions that are consummated immediately such as deliver of on-line information for payment vis-a vis transactions in which delivery is at a later date. The former may be associated with micro payments while the later supports large payments.
- Means of Settlement: Items of tokens delivered for payment must be backed by traditional forms of money or money substitutes. These may include; cash, credit which may come from banks or other traditional lending agencies such as through bank cards, credit cards and debit cards or electronic funds transfer.
- Operational Characteristics: This has to do with whether the payment systems are on-line or off-line. That is to say the customer has to be on an active on-line connection to a financial institution or other third party to validate payment whenever he wants to consummate a transaction. Similarly, another operational issue is whether the customer and merchant need to have a pre-existing business relationship or will the payment system support impulse buying. For example, does the customer need to have a key certificate before using the system and then does the user of a token pay for it. In terms of payment, prepayment is used in smart cards and electronic purse that store money by debiting the user's account at the time of the transaction. On the other hand, the user can pay on a credit or postpaid basis. That is to say, the payment is made at some time after the transaction. Credit cards and electronic cheques are used for this type of arrangement.
- Privacy and Security: Here, we need to talk about how much security and level of privacy the payment system provides or guarantees. Can there be a provision for an audit trail for all transactions and what happens when a token is lost? What about the secrecy of the content and the issues of authentication and non-repudiation? These

matters would have to be addressed in on-line payment systems.
- Who takes the risks: This has to do with the direction the risk will go, the customer or the merchant. Who takes what risk? Supposing the delivery was not made or unsatisfactory.

Some of these issues raised need a good attention for any form of on-line system to be quite effective.

**Classification of on-line payment systems**

We have several types of on-line electronic payment systems already developed, even though; some of them are yet to enjoy general acceptability. We can classify these payment systems into the following groups:
- Credit Card Based Systems
- Electronic Cheques
- Electronic Cash Payment Systems
- Electronic Micro Payment Systems

- **Credit Card Based Systems:** Some examples of this system include; Virtual PIN, CARI, Cybercast, secure electronic transaction (SET), smart cards, secure electronic payment protocol (SEPP) etc. We shall look at these very briefly, except the SET system that we may give a wider coverage.
- **Virtual PIN:** This was developed by the First Virtual Holding Inc. in 1994. It does not involve the use of encryption. To use this type of system in settlement of financial obligations, the merchants and consumers or buyers are required to register with First Virtual Holdings. During registration, a buyer forwards his credit card details including electronic mail address and receives a pass phrase called virtual PIN thereafter. Similarly, the merchant during registration supplies his bank details to the company and in return, he obtains a merchant Virtual PIN. Having completed the registration process, periodic lodgment of proceeds would be made into the merchant's bank account by the company (First Virtual).
- **CARI:** We have this as a unique and simple system that allows physical goods to be ordered by credit cards through the World Wide Web. To use this method, a consumer must first obtain and activate a virtual credit card assigned by CARI, which will be mapped to a consumer's real credit card number and protected by a PIN. On making a request, a consumer's credit card information is forwarded to the merchant via fax, email or dial up line. Usually, the system uses a web server where vendors post a web page, which is capable of accepting orders. An order is placed by the user by sending virtual credit card, PIN and order details to the web server where the merchant's shop resides, using a web form. CARI collects the order from the web server and verifies it before forwarding it to the merchant.
- **The cyber cash:** This was launched in 1995 and uses special wallet software which enables consumers to make secure purchases using major credit cards from Cyber cash wallet is the application software that does encryption which is used by a consumer to make purchases with their credit card. Every user chooses a unique Cyber cash ID and pass phrase, which are registered with the cyber cash payment server. They are also mapped to the user's public/private key pair. Purchase messages containing a consumer's credit cards details are forwarded from a merchant through a gateway server link connected to the internet on one side and to the many banks as well as bank card transaction processor on the other side. Thereafter, the actual credit cards purchase is authorized and captured in the existing banking network. Now, the results of the transactions are forwarded back though the cyber cash gateway to the merchant who can then ship the goods to the consumer.
- **The Secure Electronic transactions (SET):** This is a payment protocol that is becoming one of the most acceptable and functional means of settling business transactions using the online payment system. It is sponsored by Master card international and visa international in conjunction with some other technology based organizations such as Microsoft, Netscape, IBM etc. The SET is an arrangement whereby customers and merchants can use bankcards to settle business transactions on the Internet. It was announced in 1996 and uses RSA public-key as well as DES single-key encryption technology. The SET establishes a single technical standard for protecting payment cards purchases made over the Internet and other open networks. The features of Secure Electronic Transactions include: Confidentiality of information Integrity of data Consumer account Authentication Merchant authentication and interoperability
- **Electronic Cheques:** Paper cheques are no longer fashionable with the result that in some countries of the world, there is a decline in using them. To support this assertion, Kalokata and Whinston had observed that banks now favor inter-bank transfer and debit cards to the use of paper cheques. The major reason for this decline include the cost of processing the large volume of paper cheques and transporting cheques and transporting cheques and transporting cheques to the bank for payment to be made, as well as the expenses of returned cheques. Although Electronic cheques work in similar way to their paper cheque counter parts, yet they seem to have more flexibility in handling since it is being conveyed across computer networks. For instance, when a payer issues a cheque much like the paper cheque, it is assumed that users are enrolled in some kind of public key based identity scheme. Now, once registered; a consumer can contact a seller of goods. Arrangement within this payment system may include: Net bill; Net cheque; Electronic bill presentation and payment (EBPP), and Integrator Financial Network (IFN).
- **Electronic cash payment systems:** Payment through cash had remained the most prevalent form of settlement of financial obligations in consumer transaction. This is because the method seems easier and more acceptable as no paper trail or an additional charge for its use is involved the way it is with other payment methods. Today, some electronic cash payment systems have been developed. Suffice it to say that the electronic cash systems so developed did not have all the properties of payment

through physical cash. Incidentally, the banking industry is yet to fully embrace this new technology in its operations for some obvious reasons. The most popular among the electronic cash payment system include: Digital Cash (E-Cash), Net Cash, Cyber coin.

- **Electronic micro payment systems:** We have classes of goods and services that require the ability to pay in increment of less than the smallest coin value. A good example is the stock quoted in the stock market. The form of arrangement is regarded as micro payment as other forms of payment already discussed cannot adequately handle such transactions. Some examples of the micro payment systems already developed include: Millicent, subscript, Pay word and micro mint.
- **Millicent:** This is designed to allow payment as low as a tenth of a cent to be made. The electronic currency is called scrip. The scrip is vendor specific and has value at one vendor only. The three main entities of this system are the broker, vendor and customers. Again, the system uses no public key cryptography and it is optimized for repeated micro payments to the same vendor.
- **Pay word:** This is another form of micro payment system. It is a credit-based system that aims to reduce the number of public key operations required per payment. It does this by using chains of hash values to represent user credit within the system. When, a pay word hash value is sent to merchant. This would require the user to digitally sign a commitment to honour payments for the chain. Finally, it is the duty of brokers to mediate between users and vendors so as to maintain accounts for the two parties.

**E-Fraud**

Numerous definitions of e-fraud have been advanced in the e crimes literature. Graham defines e-fraud as "a fraudulent behavior connected with computerization by which some one intends to gain dishonest advantage". In this definition e-fraud equates to, and supersedes, the term computer fraud. Some definitions specify e-fraud in relation to electronic commerce or the Internet such as Smith in which e-fraud is seen as "any dishonest activity that involves the Internet as the target or means of obtaining some financial reward". It is also defined in relation to the Internet as "a fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme".

As it relates to electronic payments, fraud occurs in three main forms: "friendly," internal and external. Friendly fraud refers to when an individual purchases goods or services with the intention of using consumer-friendly rules to get out of paying for them. External fraud occurs when a customer provides a merchant with false information, e.g., a fraudulent credit-card number. Internal fraud is when a trusted employee steals from the merchant through various techniques. Further it is described briefly:

**Friendly fraud**

In a self-storage environment, friendly fraud is not likely. Your greatest defense is you have the ultimate control to access a customer's unit if payment is not valid. Your biggest risk is at the end of the lease when you relinquish a tenant's goods. At this point, the customer can file a chargeback claim, and you must be prepared to respond to an inquiry or chargeback issuance from the payment processor. If possible, get an electronic swipe of the card if it's a credit card or ask for a debit card instead. When a credit card is keyed in rather than swiped on a terminal, never assume the charge will survive a chargeback—it won't.

**External Fraud**

External fraud will also have minimal impact on a storage operator. The presentation of a stolen card for a recurring charge like rent is rare. This is because, on average, the rightful cardholder will be aware of any unauthorized activity within 45 days and cancel the card. In most cases, this occurs within days of it being stolen or lost.

**Internal Fraud**

Internal fraud, happens when an employee with access to the payment system abuses the privilege to steal money. Internal fraud can go on for years before it is discovered. Many experts in the payment industry believe the majority of these cases are never exposed. The most common form of internal fraud is the issuing of inappropriate credits. For example, an employee might issue a credit to a friend's credit card against a merchant charge that never occurred or issue a credit in excess of the original charge amount. He might also issue a partial or complete credit to a customer with the intention of charging less for rent or retail product than he should.

Traditionally, experts believed it rare to see external hackers committing fraud. Insider attacks are considered more "insidious" and therefore more difficult to detect. However AusCert has shown that threats of e-crime from external sources are increasing, and over-shadowing internal threats in terms of frequency and severity of incidents and opportunities for externally sourced frauds to occur. A key point to note is confusion over the treatment of former employees and contractors as both "external" and "internal" threats. Recent trends in outsourcing are likely to exacerbate these issues in regard to the level of authority or access to sensitive information. These three dimensions can be considered within the process of an e-fraud, and are seen to constitute key elements of that process, in that every e-fraud must include a perpetrator who sets out to defraud a target, which if the attacker is successful, will lead to some form of impact.

**Model of e-fraud**

Technology has a huge role in e-fraud. Technology is seen as both a target of an e-fraud and / or the means by which it is committed. To address this, two new elements are added to the model, *Mode of Attack* and *Target System*. The new elements allow various aspects of the existing elements to be adjusted to present a more consistent model in which each element has a clearer focus. The elements of this model are discussed below:

**Mode of attack**

Modes of attack are the "mechanism" used to commit fraud. Two broad types are technical and non-technical modes. Non

technical methods include identity deception (simple case of lying) and social engineering. Technical modes of attack are numerous and contribute towards the 'e' portion of the term, at times, closely related to the target system. Examples of modes of attack include data modification in systems, IP spoofing and use of malicious code. Special attention should be paid to identity fraud, as it may be either technical or non-technical. The addition of a "Mode of Attack" element allows the means by which a target may be attacked to be considered separately from both the perpetrators undertaking the attack and the system being attacked, thus assisting in clarifying the role of mechanisms to thwart various modes of attack. In addition, the rapid rate of technological development of computing as a whole can be monitored for emerging "Modes of Attack" separately from other technological aspects, such as target systems.

**Target System**

The target system element represents the system through which the fraud will be carry out. The target system includes a number of inter-connected systems, some of which may not be owned or controlled by the target entity. Systems that are wholly contained within the entity will presumably be attacked by a different type of perpetrator, using different modes of attack than those that would be used against inter-organizational systems (IOS) that are only partially controlled by the organizations. The inclusion of IOS and e-business systems must improve the prospects of a better understanding of the risk exposure that the systems on which entities rely represent. This parathion of target system from target entity allows for a clearer role for the characteristics of the system in determining the possible e-fraud threats, modes of attack, and counter measures. In addition the rapid rate of technological change in the system time; however the characteristic of organizations or individuals that causes risks may not). The separation should help strengthen the awareness of security weaknesses in the "system" itself, which are often common across organizations and distinguished from weaknesses in the organization itself (such as the inadequate control mechanisms and poor user/management awareness).

**Impact**

Impact is the result of an e-fraud incident, and may include either financial losses or nonfinancial losses. Financial losses include the cost of rectifying the situation or actual losses from assets stolen or damaged,. Non-financial losses include loss of reputation, loss of competitive advantage and personal distress and loss of wellbeing. Impact is considered separately from target entity as a single incident of e-fraud may have abroad impact across more than just the target entity or entities. This distinction accommodates for any flow on affects where the imp act can be an interim result of another 'crime' such as identity theft.

**Prevention of e-fraud pyaments: audit procedures**

With these tactics in mind, it's imperative that you have a specific set of audit procedures to monitor payment activities. Following is a recommended six-step protocol to reduce merchant-service fraud. When possible, separate and rotate these activities, and conduct audits on a random but frequent basis:

1. Understand the merchant-service statement.
2. Control all voids.
3. Investigate all charge-backs.
4. Monitor all credits.
5. Look for patterns.

**Understand the merchant-service statement**

You should have a solid understanding of the basic elements of your merchant-service statement. These include the statement cycle, format, location of specific information and terminology. The statement should never be mailed to the facility office but to an off-site location where independent monitoring can occur. If you aren't comfortable monitoring your own statement, hire a payment professional to assist.

**Control all voids**

When possible, require a manager to authorize and verify every void before issuance, and independently monitor the components of each. The following information should be recorded: the reason for the void, the employee who issued it, the date and time of the void, all the associated receipts, and the signature of the customer to whom the void was issued.

**Investigate all charge-backs**

Handle charge-backs similarly to voids. For each, log the reason it occurred, the employee who initiated the sale, the date and time of sale, and the credit-card number from which the chargeback derived. You should develop a detailed information trail on all chargeback activity, auditing each one not only from the perspective of the particular event, but looking to see if a larger system or organizational issue needs to be addressed.

**Monitor all credits**

The same type of log is necessary for all credits. Make note of the reason for the credit, the employee who issued it, the employee who made the sale, the date and time of the sale and credit, and the account number used for the initial payment. This information must match the account for which the credit is issued. You'll also need the signature and phone number of the customer for auditing purposes.

**Look for patterns**

This is singularly important. Often a pattern emerges in void, chargeback and credit activity, and this should prompt a detailed evaluation. To establish a base pattern for the business, review the last six months of merchant-service statements, tabulating norms. Make careful note of the following:

- Percentage of downgrades
- Types of downgrades
- Percentage of each downgrade type
- Percentage of charge-backs
- Percentage of voids
- Percentage of credits
- Percentage of transactions by card type

To determine the meaning of any pattern, you'll need a set of benchmarks against which to compare data. Establishing those

takes a lot of work, but it's a assured way to reduce internal fraud. If you don't wish to do this yourself, hire a consultant with the experience necessary to handle the task. Ask the vendor about his experience, which database he uses, and whether the database contains information regarding your specific payment processor and market (geography and business type). Vigilance is the key to preventing lost profit in any business. Use these auditing procedures, and you'll reduce the likelihood of friendly, external and internal fraud.

**Conclusion**

E-fraud needs to be well understood to in order to properly quantify and mitigate the risk exposure. There is a need to see dimensions, the breadth and depth of e-fraud. The model presented should assist practitioners to gain a wider view of how organizations and individuals can be affected by e-fraud. A key point that arises out of the study of dimensions of e-fraud was the prevalence of discussion of identity-related frauds implicitly and explicitly. Firstly, much of the literature identified identity fraud as a category of e-fraud or e-crime explicitly. In many cases identity related crimes were implicit in nature, for example, many white-collar crimes were committed through the use of 'borrowed' or stolen identities and passwords. It would seem that identity fraud and e-fraud are intimately linked and further research into the nature of this relationship seems important to a better understanding of e-fraud. Another implication for the model is that in the future this model may help facilitate a better collection of more detailed data and by using a richer data set across the various dimensions identified in the model, practitioners should be able to better evaluate the risks, and by using the different perspective that make up the elements of the model, work up and down the model. The discussion of the elements of the model suggest that the model allows for the individual elements to be adequately considered in their own right which also encourages the flow-on effects and relationships between elements to be considered. The use of procedures now needs to be practiced in the field to reduce the likelihood of friendly, external and internal fraud in electronic payment system.

**References**


1. Manning R. Electronic Commerce on the Internet" in Olumide, S. A and Falaki. SO. Electronic Commerce – Promises, Treats, Trust and payment Systems, 1998-2001.
2. Wortington T. Internet Payments for Government Agencies Commonwealth of Australia, 2000.
3. Adeola FO, Falaki SO. An encryption/decryption software package based on enhance dvigenerecip her scheme, proceedings of the 14th National Conference of Computer Association of Nigeria. 1998; 9.
4. Rivest RL, Shamir A, Alderman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Comm. ACM. Schnorr, C. 1978; 21:294-299.
5. Kalokata R, Whinston A. Electronic Payment System, Addison Wesley, Reading, M ass, 1997.
6. Graham T. Dispute resolution: E-Fraud and Jurisdiction, viewed, 2002.
7. Graycar A, Smith R. Inquiry into Fraud and Electronic Commerce: Emerging trends and best practice responses, Parliament of Victoria Drugs and Crime Prevention Committee, viewed. 2002, 2003.
8. Malakedsuwan. Stevens A Model of E-Fraud 7th Pacific Asia Conference on Information Systems, Adelaide, South Australia, 2003.
9. Aus Cert. Australian Computer Crime and Security Survey, Aus Cert, Deloitte Touche Tohmatsu, NSW Police, viewed. 2002, 2003.
10. International Journal of Computer Applications (0975 – 8887). 2011, 25.
11. Rachana, Priyanka Singh. Issues and Challenges of Electronic Payment Systems, International Journal for Research in Management and Pharmacy. 2013; 2(9):25-30.
12. Bhasker, Bharat. Electronic Commerce, Framework, Technologies and Applications, McGraw Hill Education (India) Private Limited. 2013; 9.2-9.16.