Combating E-Fraud on Electronic Payment System

K. A. Akintoye
Dept of Computer Studies,
The Federal Polytechnic,
P.M.B 5351, Ado-Ekiti,
Ekiti State Nigeria

O. I. Araoye
Dept of Computer Studies,
The Federal Polytechnic,
P.M.B 5351, Ado-Ekiti,
Ekiti State Nigeria

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. 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 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 countermeasures.

Keywords
Electronic fraud, Electronic business, Electronic crime, Fraud, Identity fraud

1. 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 aegis of Network technologies. Manning [1] and Wortington [2] had observed that electronic payment transactions have been in use for several years, even the automatic teller machines (ATM), Credit and Debit cards, 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 off-line. 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.

1.1 On-line Payment Systems
The characteristic features of on-line payment systems include:

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

1.1.1 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

I) 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.

(a) 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) [3].

(b) 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, e-mail 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.

(c) 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.

(d) 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 on-line 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, [4].

The features of Secure Electronic Transactions include:

Confidentiality of information

Integrity of data

Consumer account

Authentication

Merchant authentication and interoperability

II). 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 [5] 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: Netbill; Netcheque; Electronic bill presentation and payment (EBPP), and Integrator Financial Network (IFN).

III). 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, Mondex and CAFÉ (Condition Access for Europe) [3].

IV). 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.

(a) 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.

(b) 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.

2. E-FRAUD

Numerous definitions of e-fraud have been advanced in the e-crimes literature. Graham [6] defines e-fraud as "a fraudulent behaviour connected with computerization by which someone 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". The USA Department of Justice also defines e-fraud 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" [7].

The variations in the definitions of e-fraud are attributable to a number of factors such as the differing contexts in which e-fraud has been found to occur: for example, the definition given by the USA Department of Justice [7] is consumer oriented. The perceived importance and role of the Internet / technology is other source of variation. In considering the underlying dimensions, domain and outcome differences as well as the differences in how the involvement of technology in the electronic crime is defined, numerous different definitions result. These variations are accommodated within the broad definition put forward by Graham [6].

2.1 Current Classification of E-Fraud

The variations in the definitions have resulted in considerable differences in manner by which incidents of e-fraud are classified. Much of the variation in classification schemes would appear to be the result of the differing perspectives taken by various studies. For example Graycar & Smith [8] adopted a victim's point of view in classifying e-fraud, the United States Department of Justice [7] takes a consumers view and KPMG [9] take the view of the perpetrators. A review of the various schemes uncovers a number of inconsistencies in the classifications, but more importantly reveals, through the lack of consistency and differing, but compelling perspectives, an absence of an overall model or framework of e-fraud. By creating an underlying structure upon which the existing studies may be reformulated, the disparate perspectives and classification schemes should afford reconciliation, thus creating a sound basis from which to move forward in understanding and responding to e-fraud.

2.2. Towards a Model of E-Fraud

Any crime is a result of intersection of three factors, a supply of motivated attackers, availability of target and absence of capable guardian [8]. In considering these factors, there are a number of underlying dimensions for the different areas of e-fraud that helps categorize the types and risks of e-fraud. A theory of Internet Fraud speaks of opportunity, motivation, rationalization and lack of capable guardian [8]. Starting with the differing perspectives identified from the variation in e-fraud definitions, further analysis reveals three common perspectives from which e-fraud is addressed, being:

- Target view
- Perpetrator view
- Impact view.
-

Each of these perspectives has one or more foci around which the categorizations of factors within that perspective relate. These three perspectives roughly equate to Smith & Urbas's [8] 'needs' concerning theory of Internet fraud.

The target view looks at e-fraud through the eyes of the intended targets (or victims – if the fraud is successful). Two key foci emerge from the literature in regard to this perspective. Firstly, the type of entity is seen as a main differentiating factor in the types of e-fraud risks depends on whether it is committed against individuals or against companies. Frauds against individuals most likely require different solutions to those committed against companies.

Secondly, the level of understanding of the risks or lack of knowledge of technologies can be seen to be a cause for many e-fraud incidences. This is particularly evident in the case of Malakedsuwan [10] scams targeted against individuals, in which there is a lack of 'capable guardians. Within the organizational context, lack of education incorporates insufficient governance to protect the interests of individuals or entities.

The perpetrator view looks at e-fraud through the eyes of perpetrator and is concerned with who is undertaking the frauds. Two key foci emerge in regard this perspective; the level of authority of the perpetrator is of concern and the level of skill of the perpetrator. The level of authority can be seen as a continuum as shown in figure 1.

The continuum ranges from None, in which the perpetrator is a member of the public, outside the organization and without any particular initial privileges in regard to the systems under attack, through to administrator, where the perpetrator is in a position of considerable trust and responsibility with the organization, so much so, that they are often capable of covering/disguising their actions by misappropriating the assistance of others under their supervision. At this level, such a perpetrator has complete and unfettered access to the resources required to undertake the fraud. Traditionally, experts believed it rare to see external hackers committing fraud [11]. Insider attacks are considered more 'insidious' and therefore more difficult to detect. However AusCert [11] 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.

The level of skill of the perpetrator is the other focus within this perspective. The method (and complexity of method) of attack can be seen as proxy for the skill level. It is important to note that skill level does not only refer to technical skills, but also to other skills, such as the social engineering of passwords. The levels of skills presumably could range from the ability to steal another co-worker's password from a post-it note to the hacking of a webserver and circumvention of authentication and authorization systems by breaking the encryption codes.

Finally, the impact perspective looks at the outcomes to the individual or organization of an e-fraud, should it succeed. These outcomes are often evaluated by the level of financial impact e-fraud has in the financial value of e-fraud risk, although non-financial measures are also seen as applicable. Inherent difficulties in the identification of the extent of actual impacts and the measurement of both tangible and intangible impacts are noted to have implications as to how the organization (or individual) treats the threat of e-fraud.

These three dimensions can be considered within the process (or perpetration) 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 perpetrator is successful, will lead to some form of impact, as set out in figure 2.

3. A REVISED MODEL OF E-FRAUD

The above preliminary model of e-fraud is deficient as it lacks a clear identification of role of technology in the fraud, where technology is seen as both a target of an e-fraud and / or the means by which it is committed. To address this deficiency, two new elements are added to the model, *Mode of Attack* and *Target System* (which are discussed below). The elements of the process now fit together as set out in figure 3.

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 the revised model are discussed below:
The elements of the revised model are discussed below:

3.1 Perpetrator

The perpetrator or attacker in any e-fraud event will be either 'internal' or 'external' to the organization. Where the target entity is an individual, then presumably all perpetrators will be external, although this highlights the need to be quite careful when defining what is implied by entity, and hence the use of the term entity, rather than organization. Presumably an entity could be a 'family', thus allowing a perpetrator to be considered 'internal' where they have a close relationship with the family (or are part of the family) and / or intimately aware of the systems in use by family members.
The introduction of the *target system* element allows the relationship between the perpetrator and the target system to be considered separately to the relationship between the perpetrator and the target entity, thus allowing for a better understanding of how perpetrators come to understand, explore and exploit a target.

The skill level of the perpetrator now takes on two clear aspects. Firstly a perpetrator will have a particular skill level with regard to a mode of attack that they use to exploit a weakness in a target system. Secondly, they will have an understanding of how to exploit the weakness in the target system.

3.2 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 [12]. 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.

3.3 Target System

The target system element represents the system through which the fraud will be perpetrated. 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. The separation 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 countermeasures. In addition the rapid rate of technological change in the system can be specifically addressed (the technology may change over 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).

3.4 Target Entity

The separation of the target entity from the target system allows the characteristics of the entity's context to be considered without the compounding influence of the systems and distinguishes weaknesses of the technology from the entity characteristics. Entities can be divided into two classes: individuals and organizations. These class share many features (such as lack of awareness) but organizational features such as the existence control systems such as corporate governance, teams of fraud specialists, as well as prevention and detection procedures suggest that these two target groups need to be considered separately.

3.5 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, [10]. 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 a broad impact across more than just the target entity or entities. This distinction accommodates for any flow on affects where the impact can be an interim result of another 'crime' such as identity theft.

4. 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 [7], [6]. 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 revised 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 model now needs to be tested in the field for both validity in describing the process of e-fraud and, once the validity is established, its usefulness in assisting practitioners and researchers to better understand and combat e-fraud, most especially in electronic payment system.

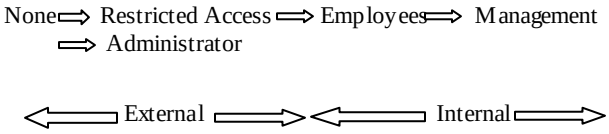

Figure 1: Continuum of Authority

Figure 2: Preliminary model of e-fraud

(source: *Malakedsuwan & Stevens A Model of E-Fraud 7th Pacific Asia Conference on Information Systems, 10-13 July 2003, Adelaide, South Australia Page 24)*

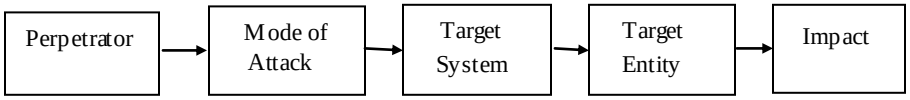

Figure 3: Revised e-fraud model

5. REFERENCES

[1] Manning, R. (1998); "Electronic Commerce on the Internet" in Olumide, S. A and Falaki, S. O (2001): Electronic Commerce – Promises, Treats, Trust and payment Systems. Conference Proceedings, Computer Association of Nigeria (COAN)

[2] Wortington, T. (2000); "Internet Payments for Government Agencies Commonwealth of Australia, *http://about.Business.gov.au/ipp/ipga.html*

[3] Adeola F.O and Falaki S.O (1998); "An encryption/decryption software package based on enhanced vigenere cipher scheme", proceedings of the 14th National Conference of Computer Association of Nigeria – vol. 9 pp 57

[4] Rivest R. L, Shamir A. and Alderman L. (1978); **"**A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm.ACM, vol. 21 pp 294-299 Schnorr, C.

[5] Kalokata, R. and Whinston, A. (1997), " Electronic Payment System", Addison Wesley, Reading, Mass

[6] Graham, T (2002), 'Dispute resolution: E-Fraud and Jurisdiction', viewed 4 February 2002, http://www.tjguk.com/topical/litigation/efraud_and_jurisdiction_winter2001.html

[7] DOJ (2001a), 'Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost $8 Million in Cisco Stock to Themselves', United States Department of Justice (DOJ), viewed 4 February 2003, http://www.cybercrime.gov/Osowski_TangSent.htm

[8] Graycar, A & Smith, R (2002), 'Inquiry into Fraud and Electronic Commerce: Emerging trends and best practice responses', Parliament Of Victoria Drugs and Crime Prevention Committee, viewed 1 February 2003, <http://www.parliament.vic.gov.au/dcpc/Reports%20in%20PDF/Fraud%20Report_final_www.pdf>

[9] KPMG (2000), 'E-commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation', Forensic and Litigation Services, KPMG LLP, USA, viewed 3 February 2003, <http://www.kpmg.com/Rut2000_prod/Documents/9/Cybercrime.pdf>

[10] Malakedsuwan & Stevens A Model of E-Fraud 7th Pacific Asia Conference on Information Systems, 10-13 July 2003, Adelaide, South Australia

[11] AusCert (2002), '2002 Australian Computer Crime and Security Survey', AusCert, Deloitte Touche Tohmatsu, NSW Police, viewed 31 January 2003, http://www.AusCert.org.au/Information/AusCert_info/2002cs.pdf

[12] Alexander, M (1996), 'The Underground Guide to Computer Security', Addison-Wesley Publishing Company, Reading, USA