**Jurnal InFestasi**
*Vol. 8 No.2 Desember 2012*
*Hal. 219 - 226*

# *ONLINE CREDIT CARD FRAUD: AN EMERGING CRIME IN THE INFORMATION TECHNOLOGY*

**Anita Carolina**

Program Studi Akuntansi, Fakultas Ekonomi, Universitas Trunojoyo Madura
Jl. Raya Telang Po.Box. 02 Kamal, Bangkalan-Madura
Email: nietaff@yahoo.com

**ABSTRACT**

*While the online retailing environment has provided businesses with an unparalleled opportunity to expand and improve their profits, it has also increased the vulnerability of businesses to online credit card fraud. This paper discusses the vulnerability of online credit card payment and the risks faced by participants in online credit card payment. As well as examining the prevalence of online credit card fraud, this paper considers strategies to reduce the risk of online credit card fraud.*

***Keywords***: *Online Payment, Credit Card Fraud, Prevention.*

## INTRODUCTION

The Internet has taken its place as an important part of people's lives. Consumers rely on the Internet to shop, bank and invest online. Most online hoppers use credit cards to pay for their purchases. As credit card becomes the most popular mode of payment, cases of fraud associated with it are also increasing. The incidence of consumer credit card fraud has been on the increase worldwide over the past few years. In the UK alone, the cost of credit card fraud totaled £428 million for 2007 (APACS, 2008). Meanwhile in Australia, credit card fraud costs Australian business 100 million dollars annually. This paper will discuss methods of electronic payment using credit card, techniques of online credit card fraud and the risks faced by participants in online credit card payment. As well as examining the prevalence of online credit card fraud, this paper considers strategies to minimize the risk of online credit card fraud.

### 1. Electronic Payment System

An electronic payment system is any kind of network service that includes the exchange of money for goods or services. Electronic payment systems can be broadly categorised as follows (Australian High Tech Crime Centre, 2007):

a. *Software-based* or *hardware-based*: software-based money includes virtual currency as used in online games with large numbers of players. Hardware-based money (or card money) includes bank driven and backed key stored value systems.
b. *Online-based* or *offline-based* schemes (based on the type of payment validation): in online schemes (e.g. BPay), issuing banks must be contacted at the point of purchase to provide authorisation when payments are made. Offline-based schemes, on the other hand, provide offline authorisation capability where validation is made based on information contained on the card.
c. *Picopayment*, *micropayment* or *macropayment* systems (depending on the dollar amount of transactions): When large amounts of

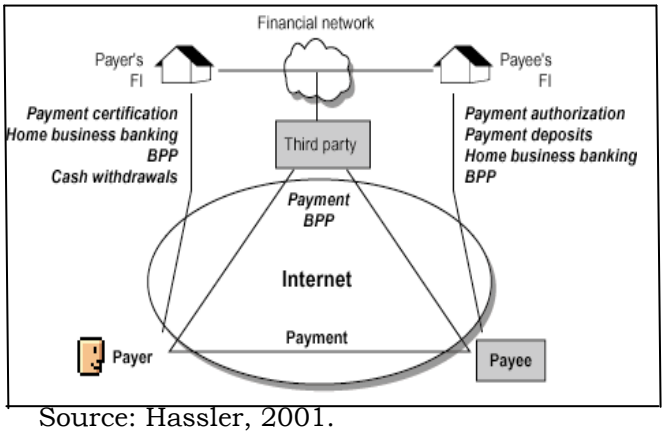
money are exchanged it is called a *macropayment* system, and small payments involve a *picopayment* system and a *micropayment* system. *Macropayment* systems need a higher level of security and non-repudiation of transactions. Meanwhile, to be viable, *picopayment* and micropayment systems need to be efficient, low-cost and secure (Hassler, 2001).

The electronic payment system involves several participants including, payer and payees, banks or financial institution, third party non banking financial institution, and financial networks (Hassler, 2001). The roles of the participants in an electronic payment system can be summarized as:

1) *Payers and Payees:* Make or receive payments (payers and payees can be individuals or organizations).
2) *Banks or financial institutions:* Hold accounts for payers and payees.
3) *Third-party nonbanking financial institutions:* Provide payment services and interface with financial networks to activate transactions against accounts held in banks (CyberCash is an example of a third-party nonbanking institution).
4) *Financial networks:* Interconnect banks to each other and with third-party nonbank financial institutions. (MasterCard and Visa run credit-card networks designed for realtime payment authorization, whereas the Automated Clearing House (ACH) and wire transfer networks focus on batch clearing of transfers between accounts)

Figure 1 below shows one scenario of participants in an electronic payment system.

Figure 1.
Participants in An Electronic Payment System




Source: Hassler, 2001.

### 1.1. Electronic Payment Using Credit Card

Credit cards have become the defacto standard for all online payments. Promises of cybercash, digitalcheques, smart cards and other alternative online payment mechanisms have largely been unrealised. Credit cards are a payment mechanism people understand and are comfortable using. *"A credit card is a card that allows you to borrow money to pay for things. There will be a limit to how much you can spend called your credit limit. At the end of each month you can either pay off the whole of the amount you owe or make a minimum repayment"* (Prof. Phill Edwards, as cited in in Gundomoni & Dara, 2006).

Credit cards generally known as plastic cards are widespread and their use for online payments is increasing dramatically. It is believed to be a magic card that offers enormous solutions for the many difficulties created by conventional payment. Unfortunately, credit cards have become the new target in cybercrime where fraudsters utilise advanced technologies to manipulate, deceive, and fraudulently use credit cards for their illegal economic gains. That is, to obtain goods without paying, or to obtain unauthorized funds from an account. Electronic payment using credit cards, which have been adopted in countries worldwide, are typically used for micropayments in view of their

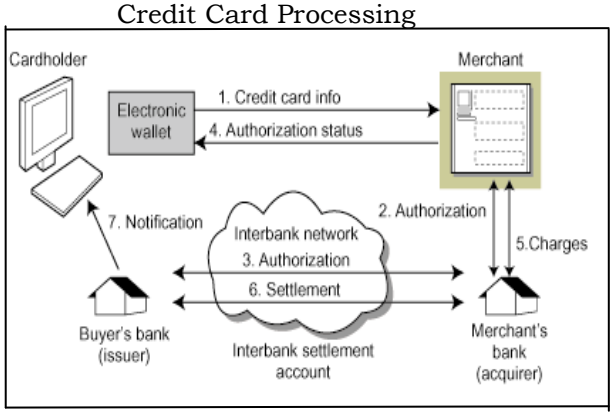
limited storage capacity (Australian Institute of Criminology, 2007). Unlike paper money, the usage of a credit card is not identifiable and it is difficult to trace.

### 1.2. Credit Card Processing

Processing online credit card transactions is the same as face-to-face credit card transactions, except that the online transactions have to be routed through payment networks. The typical steps to process an electronic transaction involving credit cards are:

1. Buyer sends payment information to the merchant server. Merchant software must send and receive messages; encrypt and decrypt; store public and private keys; and request and receive certificates.
2. Merchant software takes payment information from the cardholder and sends it to the acquirer (merchant's bank). Acquirer institution must receive and authenticate payment information the merchant received from the cardholder.
3. Acquirer sends an authorization request to the issuer over the interbank network. Issuer sends the authorization response to acquirer.
4. Acquirer notifies merchant about the status of authorization; if the response is positive, the merchant fulfills the order.
5. The merchant presents the charge to the acquirer bank.
6. Acquirer sends a settlement request to the issuer.
7. Issuer charges the buyer's credit card account and at regular intervals notifies buyer of the transactions and accumulated charges.
8. Buyer pays the charges to the bank. Acquirer credits merchant's account.

Figure 2.
Credit Card Processing




Source: Hassler, 2001.

## 2. Credit Card Fraud

Credit card fraud occurs "When an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made." (Bhatla, Prabhu&Dua, 2003)
That is, credit card fraud or plastic card fraud, or crimes of deception committed through the use of credit card, is a fraudulent transaction where an individual is unaware of the fact that a placed order will not be paid for by the cardholder.

### 2.1. Types Of Credit Card Frauds Method

Several common ways to commit credit card fraud are as follows (Bhatla, Prabhu & Dua, 2003):

1. An act of criminal deception mislead with intent by use of unauthorized account and/or personal information
2. Illegal or unauthorized use of account for personal gain
3. Misrepresentation of account information to obtain goods and/or services.

Credit card frauds can be broadly classified into the three categories of card related fraud, merchant related fraud, and internet fraud. The different

types of methods of commiting credit card fraud are discussed below.

### 2.1.1. *Card Related Fraud*

**a. Application Fraud**

Application fraud can take two forms, *familiar* and *unfamiliar*. The *familiar* version occurs when a family member or personal acquaintance easily accesses to an individual's personal information to fill out a credit card application and use the credit card as if they were the true cardholder. Once identified, these situations are generally resolved by the individuals involved. Application fraud from an *unfamiliar* form occurs when a person unknown to the victim gains personal information about the victim, obtains a card in the individual's name and proceeds to use it without the individual's knowledge. Personal information used in the fraudulent application is secured using a variety of illegal tactics, often aided by technology. Use of the internet has made it far easier to obtain personal information used in the application processes (Buttafogo in Burns&Stanley, 2002; Bhatla, Prabhu&Dua, 2003).

**b. Lost/Stolen Cards**

This type of fraud occurs when a person legitimately loses his card or the card is stolen by an irresponsible person and used for criminal purposes. The criminal can gain direct access to the individual's credit card account and may also gain access to other personal information about the individual. This can cause complex problems if the information is used to broaden the fraud, for example by applying for other cards. This type of fraud is the simplest way for criminals to obtain another's credit card without employing modern technology (Buttafogo in Burns & Stanley, 2002; Bhatla, Prabhu & Dua, 2003).

**c. Account Takeover**

Account takeover occurs when a criminal illegally obtains a valid cardholders' personal information to effectively represent the person with the card issuing bank. The legitimate account control is taken by the fraudster by either providing the customer account number or the card number. The fraudster then contacts the card issuer, pretends to be the genuine cardholder, to report the card lost and ask for a replacement to be sent to a new address (Buttafogo in Burns & Stanley, 2002; Bhatla, Prabhu & Dua, 2003).

**d. Fake and Counterfeit Cards**

This type of fraud, together with lost/stolen cards forms are the highest number of credit card frauds. Fraudsters utilise innovative techniques to create false and counterfeit cards, for instance (Buttafogo in Burns&Stanley, 2002; Bhatla, Prabhu&Dua, 2003):

a. *Creating a fake card*: Fraudsters use sophisticated machines to create a fake and counterfeit card from scratch. Many security features are designed to protect credit cards from fraudster forge and counterfeit, such as, holograms.
b. *Erasing the magnetic strip*: Fraudsters erase the metallic strip on credit cards using a powerful electro-magnet. The details on the card then are tampered so with that they match the details of a valid card, which may have been attained fraudulently.
c. *Altering card details*: a process where fraudsters alter cards by: (1) re-embossing a credit card using heat and pressure to the information originally embossed on the card by a legitimate card manufacturer; (2) re-encoding a credit card using computer software that encodes the magnetic stripe data on the card.
d. *Skimming*: Fraudsters electronically duplicate valid data on a card's magnetic stripe onto another card by utilizing pocket skimming devices, a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to obtain a customer's card details. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters.
e. *White plastic*: fraudsters create and encode a card-size piece of plastic

with legitimate magnetic stripe data for illegal transactions. Usually fraudsters use this card at Point of Sale (POS) terminals where card validation or verification is not required (for example, petrol pumps and ATMs).

### 2.1.2. *Merchant Related Frauds*

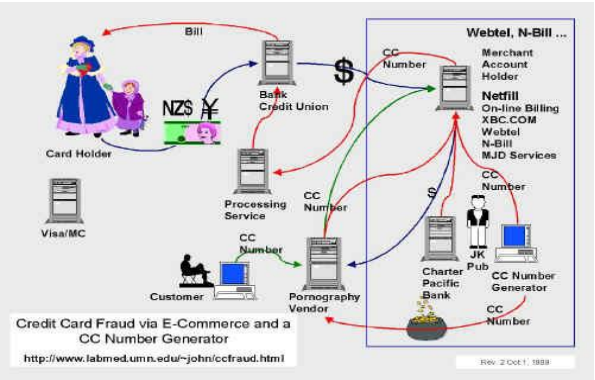
1. Merchant Collusion
   The fraudsters in this type of fraud are both the merchant owner and or their company. They conspire to fraudulently use their customer's account or personal information to commit fraud.
2. Triangulation
   Fraudsters imitate a legitimate auction or sales site to deceive card holders. Once cardholders place personal information on the site, the fraudster steals that information and uses it to order goods from a legitimate site.

### 2.1.3. Internet Related Frauds

As the Internet increases in range and wealth of business opportunities, so do criminals increase their efforts to develop more sophisticated and effective ways to scam online. Several common techniques that utilize the internet to commit credit card fraud (as summarized in figure 3) (Faughnan, 2004):

1. *Site Cloning*: almost the same as triangulation, site cloning allows fraudsters to clone an entire site or just the pages from a legitimate auction or purchase site. Customers (cardholders) do not realize they have been deceived as the cloned site is identical to the real site and the site will send a transaction receipt via email to the customer. Personal information that fraudsters receive will be used to commit credit card fraud.
2. *False Merchant Sites*: Usually these sites offer cheap services to customers or sometimes free services. However, a customer has to give personal credit card information with a reason to verify an individual's age. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.
3. *Credit Card Generators*: Credit card number generators are computer programs that generate valid credit card numbers and expiry dates. The methods used by this program is to generate lists of credit card account numbers from a single account number and use the mathematical Luhn algorithm that card issuers use to generate other valid card number combination, in the form of any of the credit card formats, such as American Express, Visa or MasterCard.
4. *Card Holder-Not- Present (CNP)*: At the same time, on-line transactions are considered "card not present" (CNP) transactions since the card was not swiped through a Point of Sale (POS). CNP fraud involves stolen card details being used to pay goods and services over the internet, by phone or by email order. Fraudsters normally obtain the details of credit card by copying without the knowledge of the card holders, collecting from the receipt thrown away by the customer or by a skimming process. The difficulty in countering this type of fraud lies in the fact that neither the card nor the cardholder is present when the transactions happen.

Figure 3:
The General Technique of Credit Card Fraud Via Internet




Source: International Net-Based Credit Card (Faughnan 2004, as cited in Gundomoni & Dara, 2006)

**3. Impact of Credit Card Frauds**

Fraud on credit and debit cards has a high cost to the card holders, the merchants, the acquirers as well as the issuers.

1. Impact of credit card fraud on cardholders
   Amongst all participants involved in credit card transaction, both card present and card not present case, cardholders are the least impacted party, due to the limitation of consumer liability for credit card transactions by the legislation prevailing in most countries. Credit card issuers have standard customer liability limitation and also have cardholder protection policy to protect cardholders from losses.
2. Impact of credit card fraud on merchant
   In the case of a fraudulent transaction, the most impacted participant in credit card fraud is the merchant merchants who offer a product or service online have to take the risk of losing the cost of the good sold, shipping cost, card association fees, merchant bank fees, administrative costs, loss of reputation, and even face the possibility of having their merchant account terminated by the financial institutions serving them. In some cases, on-line merchants will actually meet the cost of fraud personally to avoid higher charge backs and the risk of losing their merchant's licence. The Cybersource Online Fraud Report showed Internet fraud had cost merchants $2.6 billion, or 1.8% of total online revenues, in 2004.
3. Impact of credit card fraud on bank (acquirer or issuer)
   Even though the issuer or acquirer does not bear the direct cost of credit card fraud, in some cases the issuer or acquirer will be legally responsible for the cost of the fraud. In the case of charge back issued to the merchant, the acquirer or the issuer has to be responsible for administrative costs and manpower costs. In addition, the acquirer or issuer also has to invest a large amount of money to develop and deploy sophisticated IT device for prevention and detection of fraudulent transaction.

**4. Credit Card Fraud Prevention**

Preventing internet-related crime and particularly fraud will involve a wide range of strategies which extend from hard regulation involving the use of the law; soft regulation using codes of practice; and technological solution.

**1. Hard regulation**

The regulation of advertising and marketing is a relatively new phenomenon. With the introduction of advanced technology; consumer needs a strict legal prohibition of unethical practice (the so called hard regulation approach) to protect them from fraudulent transactions.

a. Civil Action
   Most of the advertising content which appears on the Internet is, legally, an invitation to buy. Interested customers will voluntarily give their personal information details including name, address and credit card account numbers. If the process to purchase is accepted and supported, it will give rise to a legally binding agreement.
   However, fraudsters can display misleading or deceptive advertisements on the Internet to deceive customers. In this case customers have no right to rescind the contract or sue for damages due to particular evidentiary and forensic difficulties associated with establishing what transpired between the parties to an electronic transaction.
b. Consumer Protection
   Consumers need a law to ensure that that consumers are not coerced into buying products which they do not want and are not otherwise deceived by sellers.
   In Australia, for instance, both federal and state consumer protection laws apply to transactions in which Australian citizens or corporations are involved. The *Trade*

*Practices Act 1974* (Cth) has provisions concerning consumer protection in Part V which proscribe various unfair practices and specify product safety standards and the operation of conditions and warranties in contracts.

c. Criminal Action
Criminal prosecution and punishment such as fines and imprisonment intends to prevent those who perpetrate offences from re-offending and also to deter others in the community from acting illegally. However, there a number of legal problems associated with proving deception carried out electronically, such as various forensic difficulties associated with gathering evidence from computers in a number of different jurisdictions (Davis, 1997, as cited in Smith, 2000).
In Australia, for example, Cybercrime Bill 2001imposes a maximum penalty of 10 years' imprisonment for offences including (s. 477.1) unauthorised computer access, (s. 477.2) modification or impairment with intent to commit a serious offence, unauthorised modification of data to cause impairment, (s. 477.3) and unauthorised impairment of electronic communication (Parliament of the Commonwealth of Australia 2001).

**2. Soft Regulation**

Considering practical difficulties associated with relying upon legislative regulatory approaches to control misleading and deceptive on-line conduct, several industry groups created self-regulatory groups which employed their own standards and codes of practice.

a. Technological Solutions
There are numerous technological solutions that can be employed to minimize the risk of credit card fraud, for instance:

b. Risk Scoring Technologies
These technologies are based on statistical models derived from the transaction characteristics in order to recognize fraudulent transactions. There are two main advantages of these technologies: (1) give the comprehensive evaluation of a transaction being captured by a single number; (2) indicate the degree of suspicion on each transaction. Transactions can be prioritized based on the risk score and given a limited capacity for manual review, only those with the highest score would be reviewed.

c. Neural Network
If one is unable to prevent on-line fraud from taking place entirely, then at least it may be possible to identify the presence of fraudulent transactions quickly in order to reduce the extent of any losses caused by credit card fraud (Smith, 2001; Bhatla, Prabhu & Dua, 2003). Neural network technology has been devised to analysis user spending patterns in order to alert individuals to the presence of unauthorised transactions and also merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants. Nestor Inc., for example, provides software called PRISM (Proactive Fraud Risk Management) which is used to detect credit card fraud such as lost cards, stolen cards, counterfeit cards, fraudulent applications, cards never received, mail order, phone order and catalogue sales and merchant fraud.

d. Biometrics
One way in which problems of password and token security may be overcome, is for users to identify themselves biometrically (Smith,2001; Bhatla, Prabhu & Dua, 2003). Biometrics technique records a unique physical characteristic of the cardholders; include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odors.

## CONCLUSION

While offering numerous advantages for transaction business, the internet also offers the possibility of

fraud in credit card transaction. There are many ways in which fraud may be committed using credit cards (Bhatla et al. 2003). The use of credit card in online payment could bring significant impact not only on cardholders but also on merchants and banks. Numerous methods are used to identify potential fraud in order to minimize prospective losses, ranging from hard regulation, soft regulation, to technological solutions.

**REFERENCES**

Bhatla, T.P., Prabhu V., Dua, A. 2003. *"Understanding Credit Card Frauds*. Tata Consultancy Services.

Dara, J., Gundemoni, L. 2003. Credit Card Security and E-Payment: Enquiry into credit card fraud in E-Payment. Information System Sciences.

Faughnan, J. International Net-Based Credit Card/Check Card Fraud with Small Charges. http://www.faughnan.com/ccfraud.html#CPBank.

Hassler, V. 2001. Security Fundamentals for E-commerce. Computer security series.

Smith, R. 1999, The Prevention of On-Line Financial Fraud. In 13th International Conference on Commercial and Financial Fraud: A Comparative Perspective. *International Society for the Reform of Criminal Law*, St Julians, Malta.

Smith, R. 1998. Plastic Card Fraud. In Crime Against Business-Conference. *Australian Institute of Criminolog*. Melbourne.

Smith, R. 1997. Card Games: Plastic Fraud and Misuse. *Australian Accountant*.

Australian High Tech Crime Centre. 2007. No. 14. http://www.aic.gov.au/publications/htcb/htcb014.pdf

Online Fraud Report, 2002-2006. Online Credit Card Report Trends and Merchant's Response. Mind Ware Research Group. Cybersource. http://www.cybersource.com

Parliament of the Commonwealth of Australia 2001. http://www.parliament.wa.gov.au.