

Consumer Protection against Unauthorized Use of Credit Cards in Malaysia:

a Banking Law Perspective.¹

Kalavathy Maruthavanar
Law Faculty, University Malaya
Kuala Lumpur, Malaysia.
E mail: kalavm@um.edu.my

Plastic cards have invaded the monetary market as a payment instrument used to purchase goods and services. There are several types of plastic cards in the circulation namely, credit cards, debit cards, charge cards, stored value cards and smart cards. The first credit card used to eliminate the need to carry cash was the Mobil Oil, USA card issued in 1914 and the first form of charge card was the Diners card, which was used by businessmen in the 1950's to purchase meals on an expense account. Since then, a variety of cards have been introduced to customers that have a multitude of functions for their daily transactional needs. The numbers of individuals that rely on cards have increased from year to year and presently the plastic card has become an indispensable instrument in the money wallet. Among all the different types of plastic cards, the most favoured by customers is the credit card. Statistics provided by Bank Negara Malaysia indicate that as at August 2007, principal card holders number 8.22 million; supplementary card holders' number 1.15 million; and in August 2007 the number of credit card transactions using (local and foreign) credit cards totaled 20.21 million.² The credit card appears to be the most favourite plastic card among Malaysians. However, the downside of owning the credit card is the danger of it being used by unauthorized third parties to illegally purchase goods/services or to withdraw moneys/credit advances from the automated teller machine. Is the consumer protected from incurring the liability of such illegal transactions? The writer will discuss the extent of legal protection afforded by banking laws in protecting innocent bank customers from being burdened with illegal transactions conducted in his name.

1. Introduction

1.1 The Definition of "Credit Cards" and "Issuers" In Payment System Act (PSA) 2003

Firstly the writer will explain the definition of "credit card" in Malaysia. The main banking statute in Malaysia is the Banking and Financial Institutions Act (hereinafter referred to as "BAFIA") which is used by our Central Bank (hereinafter referred to as "Bank Negara"). The BAFIA used to govern traditional banking as well as electronic banking. However, in 2003, amendments were made to BAFIA to delete all references to electronic banking. This was done in order to move all electronic banking provisions to a new Act that would deal solely with such transactions. The new Act is The Payment Systems Act 2003 (hereinafter referred to as PSA 2003) which came into force on 1st November 2003. The difference between BAFIA and the PSA is that BAFIA only applies to licensed banks and financial institutions where else the PSA applies to banks, financial institutions and all other forms of non-banking/finance companies that are involved in the payment system. This has actually

¹ This paper is an ongoing PhD research by the writer. Therefore it cannot be reproduced or used in any manner whatsoever without the written permission of the writer and University Malaya.

² Credit Card Operations in Malaysia, Bank Negara, Monthly Statistical Bulletin, August 2007 at p 81.

broadened the supervision power of Bank Negara that historically only supervised banks/financial institutions.

The “credit cards” have been classified as a “designated payment instrument” in the Payment Systems Act 2003. A “payment instrument” means any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to otherwise make payment.³ “Designated payment instrument” means a payment instrument prescribed as a designated payment instrument under Section 24 (1) of the aforesaid Act. Section 3 of the Act further adds that “Where an operator issues a designated payment instrument, such operator shall also comply with the requirements of Part III. Part III is titled “Payment Instruments”. Part III, contains the aforesaid Section 24 whereby pursuant to subsection (1), Bank Negara has imposed two criteria to be fulfilled before a particular instrument is classified as a “designated payment instrument”. The two criteria are as follows:

- i. That the payment instrument is of widespread use as a means of making payment and may affect the payment systems of Malaysia;⁴ and
- ii. It is necessary to protect the interest of the public or it is necessary to maintain the integrity, efficiency and reliability of a payment instrument.⁵

A credit card is of widespread use as a means of making payment by customers and apart from cash and cheques, is a popular mode of making small value payments by customers for retail purchases and services. The second criteria reflects Bank Negara’s role as the custodian of consumer protection in the credit card sector, as it regulates the payment instrument in order to protect public interest and authenticate its integrity, efficiency and reliability.

Bank Negara in exercise of the power conferred by section 24(1) PSA 2003 and its subsidiary legislation making power under section 70, made the Payment Systems (Designated Payment Instruments) Order 2003. Pursuant to paragraph 2 (b) of the said order, a credit card is a designated payment instrument. Paragraph 2 (b) of the Order states that a credit card is a payment instrument which indicates a line of credit or financing granted by the issuer to the user and where any amount of the credit utilized by the user has not been settled in full on or before a specified date, the unsettled amount may be subject to interest, profit or other charges. In other words, a credit card allows the use of credit line to the customer wherein the customer has the option either to settle in full by a stipulated date or to defer payments in the form of minimum monthly installments.

In this context, a bank that issues credit cards would be defined as an “issuer” or alternatively as an “operator”. An “issuer” means any person acting alone or under an arrangement with another person, who undertakes to be responsible for the payment obligation in respect of a payment instrument resulting from the user being issued with or using the payment instrument.⁶ An “operator” means any person, acting alone or under an arrangement with another person, responsible for the rules, procedures and operations of a payment system but excludes such persons as may be prescribed by the Bank.⁷ The PSA 2003 uses both the terms

³ Refer to Section 2, Interpretation, The Payment Systems Act 2003.

⁴ Section 24(1)(a) of the Payments System Act 2003

⁵ Id. subsection (1) (b).

⁶ Supra footnote 2.

⁷ Ibid.

of “issuer” and “operator” interchangeably (This can be noted when reading Part II, PSA 2003 which uses the term “issuer”).

The PSA 2003 through its subsidiary legislation making power conferred by section 70 has issued the most recent version of the Credit Card Guidelines (Version 2.0). This version of the guidelines supersedes all previous credit card guidelines issued in the past under the BAFIA. The aforesaid Credit Card Guidelines (Version 2.0) actually incorporates important provisions from the former credit card guidelines by giving such provisions a new ‘facelift’ in line with the move by Bank Negara to transfer all credit card provisions from BAFIA to the PSA 2003.

Paragraph 2.1.1 of the Credit Card Guidelines (Version 2.0) defines “credit card” as a payment instrument which indicates a line of credit or financing granted by the issuer to the user and where any amount of the credit utilized by the user has not been settled in full on or before a specified date the unsettled amount may be subject to interest, profit or other charges. This definition reiterates the definition of “credit card” in the above stated Payment Systems (Designated Payment Instrument) Order 2003. However the definition of “issuer” in the Credit Card guidelines is more precise than the definition given in the PSA 2003.

In paragraph 2.1.2 of the Credit Card Guidelines, “Issuer of credit card” means:

- a. A licensed institution that issues credit cards; or
- b. A person who has obtained Bank Negara Malaysia’s (BNM) approval to issue credit cards under subsection 25(1) of the PSA; and
 - (i) the line of credit is provided by a licensed institution; or
 - (ii) the issuance of the credit card is carried out through a joint venture arrangement with a licensed institution.

The term “Licensed institution” is defined in paragraph 2.1.3 of the Credit Card Guidelines as meaning any person licensed under subsection 6 (4) of the BAFIA to carry on banking business, banking and finance company or merchant banking business.

The definition of “Issuer of credit cards” and “Licensed institution” in the Credit Card Guidelines indicate that any credit card issuance or credit card financing has to be by a licensed bank/finance company either solely or together with another joint - venture entity. Therefore if an entity does not have a license issued pursuant to subsection 6(4) of the BAFIA, then it cannot carry out the credit card business in Malaysia.

As a result, the general rule is that all credit card holders in Malaysia are bank’s customers. The joint venture between local banks and Visa or MasterCard, (US) is to use the international network’s brand name and technology in the credit card business. Therefore Visa and MasterCard in Malaysia do not issue plastic credit cards and are not issuers under the PSA 2003. All local banks which subscribe to Visa or MasterCard (Malaysia) and the industry comply with the ‘first commandment’ of the payment card industry. The first commandment is to “Honour all cards”, which means merchants are not allowed to pick and choose which

cards they wish to accept.⁸ They are to accept all cards be it in blue, gold or silver colour as long as it has either the Visa or MasterCard insignia.

Another type of joint venture involves the issuance of co-branded credit cards. Co-branded credit card holders are credit cards which are issued by the credit card issuer and a merchant under a well-known brand name.⁹ The merchant offers additional benefits to the cardholders, such as discounts on certain products and reward points for purchases. The co-branded credit cards were first initiated by the airline industry for frequent travelers to collect points used to redeem gifts. The current examples of co-branded credit cards are Maybank-Sogo Visa, Public Bank-Esso, Visa RHB - Air Asia MasterCard, Citibank- Air Asia Cards. The agreement between the merchant and the issuer bank is that the merchant solely permits its brand name to be used and is not an "issuer". Therefore the merchant does not assume any legal obligation as an issuer under the PSA 2003. The issuer bank enters into such a scheme with the merchant to tap on the merchant's customer base.

The only exception to paragraph 2.1.2 of the Credit Card Guidelines is that Bank Negara can exempt an entity which is a non-bank from the requirements of that paragraph. An example of a non-bank that has been allowed to issue credit cards is AEON Credit Service M Sdn Bhd (the company that manages the Jaya Jusco stores throughout Malaysia). AEON Credit Service M Sdn Bhd is a non-bank issuer and assumes all the legal obligations as an issuer under the PSA 2003. However being a non-bank, such an entity does not fall within the purview of a financial institution as stipulated in BAFIA, and its guidelines namely the Guidelines on Consumer Protection on Electronic Funds Transfers Guidelines (BNM/GP 11).

1.2 The Common Law Description of "Credit Cards".

A credit card is a card that enables the cardholder to pay for goods and services on credit and to obtain cash advances. The English case of *Re Charge Card Services Limited*¹⁰ described the features of a credit card as follows:

- i) There is an underlying contractual scheme which predates the individual contracts of sale. Under this scheme, the supplier has agreed to accept the card in payment of the price of the goods purchased and the purchaser is entitled to use the credit card to commit the credit card company to pay the supplier;
- ii) The underlying scheme is designed primarily for use in over-the-counter sales, *ie* sales where the only connection between the retailer and purchaser is the sale transaction itself;
- iii) The actual sale and purchase of the goods is the subject of a contract made between the buyer and seller, *ie* the sale contract itself;
- iv) Since the transactions are over-the-counter sales, the card does not carry the address of the cardholder and the supplier will have no record of his address. The seller therefore has no means of tracing the purchaser except through the credit card company;

⁸ Honor All Payments, Chapter 6, Paying with Plastic, The Digital Revolution In Buying and Borrowing, David Evans and Richard Schmalensee, The MIT Press (2001), at p 119.

⁹ Refer to the banking info booklet, Card Transactions and You, Credit Cards, a consumer education programme by BNM and the Association Of Banks In Malaysia, 21 January 2003 at p 12.

¹⁰ [1986] 3 WLR 697

- v) Payment by credit card will usually be treated as absolute payment of the purchase price as between the supplier and the cardholder. Thus, if the credit card company goes into liquidation before it pays the supplier, the cardholder will not be liable to the supplier of services of goods.

The principles enunciated in the above stated English case were applied in the Malaysian cases of *Tee Thian See v PP*¹¹ and *PP v Yap Seai Hai*¹².

2. Consumer Protection Governing the Terms and Conditions of the Credit Card Scheme

2.1 Guidelines On Consumer Protection On Electronic Funds Transfers, BNM/GP 11

The consumer protection guidelines issued pursuant to BAFIA are known as “Guidelines on Consumer Protection on Electronic Funds Transfers, BNM/GP 11 (hereinafter referred to as “BNM/GP 11”). The preamble of these Guidelines states “to provide a basic framework to establish the rights, liabilities and responsibilities of customers and financial institutions relating to electronic funds transfers”. These Guidelines are issued pursuant to sections 119 (since deleted) and section 126 of BAFIA. Section 77(4) of the Payment System Act 2003 has the effect of ensuring that all guidelines on electronic banking that are issued under BAFIA continue to be valid under Payment Systems Act 2003 (even though the enabling section 119 in BAFIA has been deleted).

Part 1, paragraph 3 of BNM/GP 11 titled “Definitions” states that the definition of “Card” means any card, including an ATM card, EFTPOS card, debit card, credit card or stored value card, used by a customer to effect an electronic funds transfer. The terms and conditions of “electronic funds transfer” contract are governed by Part III of BNM/GP 11. However under the explanatory statement in paragraph 4 (about what “electronic funds transfer” means, the credit card has not been included. [Note: “debit card” and “cash dispensing machine “is included in paragraph 4(g) and (d) respectively].

This creates confusion as to whether Part III of BNM/GP 11 governs credit cards. However an examination of paragraph 6(4) of the Guidelines stipulates that the standard terms and condition of the any electronic funds transfer contract shall include:

- (a) the customer’s liability for any unauthorized electronic fund transfer and duty to report to the financial institution promptly any loss, misuse, theft or unauthorized use of, access code or a card;

The definition of “card” includes credit cards. Therefore the above stated paragraph 6(4)(a) would apply to all forms of uses of the credit card since that paragraph specifically refers to the word “card”. However the subsequent sub-paragraphs in 6(4)(b),(d)(e) and (f)¹³ do not expressly refer to the word ‘card’. Therefore the aforesaid clauses would only apply to the use of the PIN to withdraw cash advances with the credit card. This is because a PIN is an “access

¹¹ [1996]3 MLJ 209 at pp 218 & 220, this case is discussed below.

¹² [1994] 291 MLJU 1.

¹³ Paragraph 6(4)(c) specifically deals with “preauthorized electronic fund transfer”.

code"¹⁴ that can be used to access a customer's credit card account to initiate an electronic fund transfer. Furthermore, a credit card PIN is used to withdraw cash advances from a "cash dispensing machine" or in other words an ATM machine in compliance with the meaning of "electronic funds transfer" in paragraph 4(d).

Therefore BNM/GP 11 has a limited application in regulating the terms and conditions in a credit card agreement.

2.2 Credit Card Guidelines (Version 2.0), June 2000

Next, the writer will peruse the provisions of the Credit Card Guidelines that afford some protection to the consumer by regulating the terms and conditions of the credit card agreement. Unlike BNM/GP 11 that can be bought over the counter at Bank Negara, the Credit Card Guidelines is only circulated to commercial banks and non-bank issuers that have joint ventures with banks.

Paragraph 6 of the Credit Card Guidelines titled "Terms and Conditions" of the credit card scheme states that :

- 6.1.1.1 An issuer of credit cards shall specify in the terms and conditions the significant liabilities and obligations applicable to the principal and supplementary cardholder in **bold print** in its application brochures and web pages. Such terms and conditions should be described in plain language which is easily understood by the applicants.
- 6.1.1.2 An issuer of credit cards shall set up a consumer credit card service section and ensure that their customer service staffs are able to answer queries on the credit card terms and conditions. The hotlines for the customer service shall be published in brochures, monthly billing statements and web pages.

The above stated paragraph 6 is mandatory and is aimed at ensuring the consumer understands the credit card scheme and not left in the lurch upon becoming a cardholder. In addition to the aforesaid paragraph 6, the Credit Card Guidelines contain sixteen other paragraphs that specifically deal with several issues in relation with credit cards including the liability of the cardholder for lost or stolen credit cards. Unfortunately these guidelines are not readily available to the public and therefore the lay person is unaware of the protection contained in the guidelines. The lay person is unable to use the guidelines as a yardstick whilst entering into a credit card scheme with a particular issuer.

3. The Fraudulent Use of Credit Cards

3.1 Malaysia the centre of credit card fraud – Magnetic stripe cards

The most prevalent problem that had plagued credit card users is the counterfeiting, forgery or skimming of cards by third party fraudsters. This problem arose because the credit cards were inserted with magnetic stripes. The first bankcard that contained a magnetic stripe was issued

¹⁴ Paragraph 3 of BNM/GP 11 defines "Access code" as including pin, password or code which provides a means of access to customer's account for the purposes of initiating an electronic funds transfer.

by Frankin National Bank of Long Island, New York in 1951.¹⁵ Plastic cards contain between one and three magnetized tracks which permit the identification of the user and enable the user to conduct a transaction from a location distant from the central data base, such as a bank.¹⁶ Some tracks allow information to be stored for passive use only (read only) and others permit information to be introduced (read and write).¹⁷ Since credit cards could easily be counterfeited, Bank Negara issued a directive to covert all magnetic stripe credit cards to chip embedded smart cards beginning January 2005. The writer will first trace the case law in the area of magnetic stripe credit cards and then continue with the latest issue relating to chip embedded credit cards.

Malaysia became notoriously known as the centre for credit card forgery in the local case of *Ooi Chat Kat v Public Prosecutor*.¹⁸ The facts of this case are as follows: Upon receiving information on the use of a false credit card at a petrol station named Henry Shell Servicing Sdn Bhd at Damansara Endah, Kuala Lumpur, an arresting officer and two bank officers arrived at the said place. At about 6 p.m. a man got out of his car and started to fill up petrol by using a credit card. The officers approached him and then conducted a body search. They retrieved a false Visa Gold Standard Chartered Bank credit card and confiscated the petrol payment receipt after the petrol pump nozzle was replaced. The crime was investigated and the man i.e. the accused was charged under section 471 of the Penal Code. The accused was convicted by the sessions court judge and sentenced to two years imprisonment. The accused then appealed to the High Court, Kuala Lumpur against the conviction and the sentence.

The learned High Court, Augustine Paul H. dismissed the appeal. The learned judge took judicial notice that Malaysia had become the centre of credit card fraud by observing:¹⁹

“It is not denied lately, crimes involving false credit cards have increased so much that there have been reports in the local newspapers that Malaysia has become a centre for producing and distributing false credit cards. The court took judicial notice that such crimes were rampant nowadays and threatened the safety and prosperity of Malaysia’s economy. If not curbed, this would affect the economy and the country’s reputation. Thus, public interest demands that such crimes be given deterrent sentences and the mitigating factors have to be considered with the background of public interest that has to be executed.”

Another case that dealt with the criminal crime of counterfeiting credit cards is the case of *Tee Thian See v PP*²⁰. This is an interesting case whereby a US Secret Service agent was investigating the source of several counterfeit cards in New York. His investigation led him to a Malaysian residing in New York who agreed to lay a trap for the counterfeiter in Malaysia. The agent and the Malaysian then executed the plan by ordering 30 gold cards at the price of US\$1,000 per card. The Malaysian met the counterfeiter in front of Hotel Equatorial, Kuala

¹⁵ PN Grabosky, Rusell G Smith, *Crime In The Digital Age, Controlling Telecommunications And Cyberspace Illegalities*, The Federation Press, 1998 at p 154. Masuda B, *Credit Card Fraud Prevention: A Successful Retail Strategy* in Clarke R (ed) *Crime Prevention Studies*, Vol 1, Criminal Justice Press, 1993 at pp 121-34

¹⁶ Id. Rusell & Smith at p 155.

¹⁷ Ibid.

¹⁸ [2003] 5 MLJ 248

¹⁹ Ibid, at p 251 (in English) and p 261 (Bahasa Malaysia).

²⁰ [1996] 3 MLJ 209.

Lumpur and was shown 28 credit cards with specimen signatures. Subsequently the police intercepted and arrested the counterfeiter. He was charged with possession of counterfeit cards under section 467 and punishable under section 472 of the Penal Code (FMS Cap 45). The Sessions Court sentenced him to four years imprisonment and a fine in default, eight months imprisonment. The counterfeiter/accused appealed to the High Court. The High Court upheld the decision of the Sessions Court.

The learned judge of the High Court, Kuala Lumpur, Justice K.C. Vohrah applied the English case of *Re Charge Card Services Ltd*²¹, and observed that there are three parties to the transaction.²² The parties are the cardholder, the retailer and the issuer of the card. The essence of a credit card transaction is that the retailer and the cardholder have for their mutual convenience, each previously arranged to open an account with the same company (the card issuer), and agreed that any account between themselves, if the cardholder wishes, be settled by crediting the retailer and debiting the cardholder's account with the issuer of the card.

The learned judge continued as follows:²³

"In a sales transaction involving a credit card, the card holder will sign on a sales voucher after the cardholder has had his card used for imprinting on the sales voucher. The sales voucher will be in three copies: one for the cardholder, the other for the retailer and the third for the issuer. The card issuer, on receipt of the third copy, will in due course pay to the retailer the face value of the sales voucher less an agreed commission (see *Re Charge Card Services Ltd* at p 702). What the signed sales voucher does is to create a legal right in the retailer to be paid the face value of the sales voucher less an agreed commission and it is certainly a valuable security within the meaning of s 30 of the Code (sic. the Penal Code).

Thus, when any of the 28 counterfeit cards is used by a person for a credit card transaction for the purchase of goods or services, and the signature on the sales voucher is forged by him, he forges a document which purports to be a valuable security; and clearly, by his obtaining goods or services on the sale transaction through the deception, he wrongfully gains from the transaction."

The writer has also noted that such credit card sales vouchers are not 'negotiable instruments' and therefore section 24, Bills of Exchange Act 1949 on forgery of signatures is not applicable to the vouchers.

There is no specific legislation to deal with credit card fraud in Malaysia and the above stated cases are examples of incidents where the prosecutors have to resort to charging the fraudsters under the Penal Code (Cap 224, Rev Ed 1985). The Penal Code in Malaysia originated from India (during the colonial times) and was enacted before the introduction of credit cards.²⁴ Although it is wide enough to cover credit card fraud, it would be better if a specific legislation is passed to deal with the problem.²⁵

²¹ *Supra*, at footnote 10

²² *Supra*, footnote 20 at p 220

²³ *Ibid*.

²⁴ Credit Card Fraud And The Law, A.L.R. Joseph, [1993] 2 CLJ xii (Apr)

²⁵ *Ibid*.

The above stated cases prompted Bank Negara to take stringent action to prevent the fraudulent use of counterfeit cards. Recently all credit cards have been converted from the magnetic stripe cards to smart cards with an embedded chip. The incidents of fraud have been reduced but even chip embedded cards have their own vulnerabilities.

3.2 The Migration to Europay-Master-Visa (EMV) Standard Chip Cards and the Latest “Contactless” Cards.

Currently all credit cards in Malaysia are embedded with the EMV standard chip. The data is encrypted at the point of use and before it is transmitted to the bank; only the intended receiver would be able to decode the data; this prevents fraudsters from capturing any credit card details and account numbers.

Bank Negara issued an official statement dated 17 August 2005 denying a news report that the microchip for credit cards had been cloned. It assured the public that the EMV chip credit card security feature adopted by banking institutions are secure. The statement further elaborates as follows:

“For account the first half of the year 2005, statistics on credit card fraud showed that the number of cases and losses have declined by 43.2% and 33.5% respectively, compared with the same period in 2004. The EMV standards are set by the international credit card associations to curb counterfeiting fraud. Malaysia is the leading country in the region adopting EMV chip infrastructure to address counterfeit fraud.”

Although the migration from magnetic stripe cards to chip cards has reduced the incidences of fraud, it has not totally eliminated such incidents. From the consumer’s perspective, it is still important to address the following issue:

Is there any protection in law to prevent third party criminals from stealing the cardholder’s identity? This is known as identity theft. (Mails in the post from banks can be intercepted by fraudsters intent on stealing a person’s identity details. Phishing sites on the internet have also been used to trick people into revealing their credit card details.) Then the illegally acquired credit card details or a stolen credit card can be used online to purchase goods; if fraud occurs in such a situation it is known as “CNP” (Customer Not Present) fraud.

Another type of credit card recently introduced in the market is the “contactless” credit card. The customer just has to wave the credit card in front of a card reader terminal before making a purchase. This type of card stores its data in a microchip fitted with a radio antenna that is capable of transmitting the card’s data to a card reader without physical contact.²⁶ Radio Frequency Identification (RFID) technology is used with ISO 14443 standard; a contactless credit card can transmit data to a special RFID card reader when the cardholder waves his card within a few inches of the receiver.²⁷

²⁶ <http://www.contactlesscreditcards.org/> (accessed 12/10/07)

²⁷ *Ibid.*

Researchers at the University of Massachusetts conducted an experiment on 20 contactless credit cards from Visa, Mastercard and American Express; the cardholder's name and other data was being transmitted without encryption and in plain text. They could skim and store information from a card with a device the size of a couple of paperback books, which they cobbled together from readily available computer and radio components for \$150. They said that they could probably make one even smaller and cheaper: about the size of a pack of gum for less than \$50.²⁸

4. The Unauthorized Use of Credit Cards

The local cases discussed above relate to the criminal prosecution of credit card offenders under the Penal Code. This means that authorities prosecute the offence as a crime against the state. As far the consumer is concerned the, the criminal has been sent to jail and the crime perpetrated using his name has ceased. Nevertheless, the consumer would also be concerned if there are civil laws that protect him from unlawful use of his credit card details and the ensuing extent of his civil liability (if any).

The unauthorized use of the credit card in general terms means that the use of the credit card was not authorized by the cardholder. The BNM/GP 11 does not define unauthorized use or unauthorized transaction although the aforesaid terms appear in the guidelines. In the United States, the Truth In Lending Act (1968) which is the consumer protection legislation for credit card use has defined the terminology "unauthorized". "Unauthorized" means "a use of a credit card by a person, other than a cardholder, who does not have actual, implied or apparent authority for such use and from which the cardholder receives no benefit".²⁹ The US Official Staff Commentary explains further that whether such authority exists must be determined under state or other applicable law.³⁰ Nevertheless the use of the words "actual, implied or apparent authority has been criticized as confusing."³¹

Some primary cardholders have supplementary users and have been authorized to use the credit card. Therefore even if the principal cardholder may have forbidden the supplementary cardholder to use the card for a particular transaction, such use is not deemed "unauthorized". The principal cardholder is liable for charges for an unauthorized use even if a particular use has been forbidden between the cardholder and the authorized user.³²

The unauthorized use of credit cards may occur in the following instances:

- (i) The cloning, counterfeiting and forgery of credit cards; as illustrated by the Malaysian cases stated above.³³
- (ii) The "access code"³⁴ meaning the PIN number was stolen and the original credit card was used to withdraw cash advances.

²⁸ Extracted from "Researchers See Privacy Pitfalls in No-Swipe Credit Cards, John Schwartz, The New York Times, 23 October 2006; <http://www.nytimes.com/2006> (accessed on 12/10/07)

²⁹ 15 U.S.C. § 1602 (o). Refer to Regulation Z, 12 C.F.R. § 226.12 n.22

³⁰ Official State Commentary on Regulation Z § 226.12(b)(5)-2

³¹ See Mark Budnitz, Margot Saunders, Consumer Banking and Payments Law, Second Edition, National Consumer Law Center, at p 58.

³² Id. at p 59.

³³ This was a major problem with the magnetic stripe cards.

- (iii) The credit card details were stolen and used on the internet, telephone, mail or fax to order goods. This is known as the 'Card Not Present Fraud' because the merchant/retailer does not view the physical card.
- (iv) The original credit card was removed, used and then replaced without the knowledge of the cardholder. In this situation, the cardholder was neither negligent nor careless in providing an opportunity for the unauthorized use of the card.

4.1 Statutory Protection for Unauthorized Use of Credit Cards

The statutory protection for unauthorized use of credit cards in Malaysia is contained in two guidelines discussed earlier namely:

- (a) The Guidelines on Consumer Protection on Electronic Funds Transfer, which has been referred to in this paper as BNM/GP 11
- (b) The Credit Card Guidelines (Version 2.0)

The writer feels that both the guidelines should be read in light of the other and not read in isolation. However for purposes of clarity, the writer will discuss BNM/GP 11 first.

(a) Consumer Protection for Unauthorized Use in BNM/GP 11

Part V of BNM/GP 11 titled "Erroneous And Unauthorized Electronic Fund Transfer" contains paragraph 14-17 that deal with the customer's duty in the event of an unauthorized use or transfer using a credit card at point- of- sale terminals, cash dispensing machines or telephonic instruments.³⁵ It should be noted that home banking or PC banking is not covered by the scope of these guidelines.³⁶ This is evidently due to the fact that home banking was only recently introduced in Malaysia; subsequent to the implementation of these guidelines. The use of credit cards on the internet would also be regulated by another set of guidelines specifically drafted for internet banking, namely "The Minimum Provisions for Internet Banking Guidelines".

The structure provided by BNM/GP 11 to provide a grievance solving mechanism for the consumer can be divided into several components.

³⁴ "access code" is defined in BNM/GP 11 as including pin, password or code which provides a means of access to a customer's account for the purpose of initiating an electronic fund transfer.

³⁵ This Part V is read together with Paragraph 3 of BNM/GP 11 that defines the scope of gadgets covered by the terminology "electronic funds transfer" in these guidelines.

³⁶ Refer to Professor Benjamin Geva, Consumer Protection In Electronic Funds Transfers, Research Paper for Industry Canada/Office of Consumer Affairs, 21 March 2002, p 80 under topic "Consumer Protection Guidelines in Malaysia".

(i) Customer's Legal Position for Unauthorized Use or Transaction

Firstly, the consumer will not be liable for the following losses incurred as a result of unauthorized use of a credit card:³⁷

- A. not attributable to or not contributed by the customer;³⁸
- B. caused by the fraudulent or negligent conduct of officers or agents of the financial institution and other network participants including merchant;³⁹
- C. relating to a forged, faulty, expired or cancelled card;⁴⁰
- D. occurring before the customer has received the card or access code;⁴¹
- E. occurring after the customer has notified the financial institution that the card has been lost, misused, stolen, or that the access code security has been breached.⁴²

The above stated paragraph A. is a statutory incorporation of the common law duty owed by the customer to its bank. Paragraph 15(1) of BNM/GP 11 explains that a customer shall not:

- (a) directly or indirectly disclose to any person the access code of his card or any electronic device used to effect an electronic fund transfer; or
- (b) fail to take reasonable care to keep the access code secret

Paragraph 15 (1)(a) and (b) is reflected by the common law *Mac Millan*⁴³ duty which was applied in the local cheques forgery case of *United Asian Bank Bhd v Tai Soon Heng Construction Sdn Bhd*.⁴⁴ A bank's customer is to take precautionary measures not to facilitate fraud or forgery of cheques. By analogy, the *Mac Millan* principle is applied in the context of credit cards; that a bank's customer is not to facilitate fraud or forgery of credit cards. A financial institution will be absolved from all liability if it can prove that the credit card holder has breached the *Mac Millan* duty.⁴⁵

The above stated paragraph B. is self explanatory and the financial institution is vicariously liable for all fraudulent and negligent conduct of its own employees and all outsourcing agents. A fraudulent employee or agent of a merchant is also covered by paragraph B.

The above stated paragraph C. relating to forged cards has to be read in light of the earlier discussed *Mac Millan* duty not to facilitate fraud or forgery. Next it also must be read together with the recent Credit Card Guidelines (version 2.0) that does impose a maximum ceiling of RM250 for unauthorized transactions as a consequence of a lost or stolen card.⁴⁶ Fraud may occur if a credit card is lost or stolen.

³⁷ *Supra*, Benjamin Geva at p 80, who discusses this point for all forms of losses of unauthorized electronic funds transfers in Malaysia.

³⁸ Paragraph 17(1) (a) of BNM/GP11

³⁹ *Id*, refer to sub-paragraph 17(b).

⁴⁰ *Id*, refer to sub-paragraph 17(c)

⁴¹ *Id*, refer to sub-paragraph 17(d)

⁴² BNM/GP 11, at Paragraph 15(3).

⁴³ Common law case of *London Joint Stock Bank Ltd v Macmillan & Arthur* [1918] AC 777

⁴⁴ [1993] 1 MLJ 182, (Supreme Court)

⁴⁵ BNM/GP 11, at paragraph 15(2).

⁴⁶ This provision will be discussed again in the next sub-topic.

Paragraph D. is further supported by sub-paragraph 17(2) which states that if any dispute arises in relation to a customer's card, then the presumption is that the customer did not receive the card unless the financial institution can prove otherwise.

Paragraph E. is a reflection of the *Greenwood*⁴⁷ duty imposed on the bank's customer to inform the bank of any fraudulent activity involving the credit card. The common law *Greenwood* duty was approved by the Malaysian courts in the above stated cheques forgery case of *United Asian Bank*.⁴⁸ The customer should not delay notification once he has knowledge of any misuse, theft or loss of credit card or its PIN.

Paragraph 16 of BNM/GP 11 provides for the customer's liability in the event he delays formal notification. In the context of credit cards, sub-paragraph 16(a) applies; and the sub-paragraph states;

Where the customer has contributed to a loss resulting from an unauthorized transaction by, delaying notification of, lost, misused or theft of the card, or someone else knowing the access code of the card, the customer is liable for actual loss which occurred, except for:

- (a) that portion of the loss incurred on any one day which exceeds the daily transaction limit applicable to the card or account;

According to sub-paragraph 16(a), the credit card holder will only be liable until the limit of charges permitted by the bank. For example if the stolen card has a credit limit of RM15,000, and the unauthorized use exceeds the limit and amounts to RM17,000; the cardholder will only be liable until the stipulated limit of RM15,000 and is protected from forking out the excess RM2,000.

(ii) Customer's Duty To Give Notification

Paragraph 14 (1) of BNM/GP 11 imposes a mandatory duty on the consumer to report to the bank any error in his statement of account or possible unauthorized transaction in relation to his card or access code. Paragraph 14(2) adds that the notification shall be made in writing 60 days from the date of the statement of account.

The writer's criticism of the above stated paragraph is that :

- (i) The mode of informing the bank via telephone is more convenient, effective and fast. If the Bills of Exchange Act 1949 recognizes countermand of cheques via telephone or in other words an oral countermand; the same mode should be adopted by credit card notification.
- (ii) The period of 60 days from the statement of account seems such a "long" period in view of the fact that fraud had been perpetrated and may still be continuing during the 60 day period. At the surface, such a long period is beneficial to the customer but in view of paragraph 16 (discussed earlier)

⁴⁷ *Greenwood v Martins Bank* [1932] 1 KB 371.

⁴⁸ *Supra*, footnote 44.

a delay in notification by the customer, could result in liability being incurred for actual losses.

- (iii) There are no consequences stated either for compliance or breach of the "60 day" notification requirement.⁴⁹

(iii) Bank's Duty on Notification

Part IV of BNM/GP 11 titled "Duties of Financial Institution" contains Paragraphs 18 and 19 on the notification process.

Paragraph 18 stipulates that a financial institution shall provide an effective and convenient means by which a customer can notify any loss, misuse, theft or unauthorized use of a card or breach of access of security.

Accordingly most financial institutions have a hotline for lodging complaints. However the legal status of an oral complaint is debatable because of the written requirement in Paragraph 14(2).

Nevertheless Paragraph 19 seems to permit telephone notification, in the following manner :

19 (1) A financial institution shall provide procedures for acknowledging receipt of notifications including telephone notification, by a customer for loss, misuse or unauthorized use of a card or breach of access code security.

(2) The acknowledgement need not be in writing provided the financial institution has a means by which a customer can verify that he had made a notification and when such notification was made.

Subparagraph 19(2) is further mind boggling as the bank's acknowledgement can be oral ; and the burden of notification (be it oral or written) is thrown back to the consumer by his verification.

(iv) The Financial Institution's Burden of Proof

Subparagraph 14 (3) discusses the financial institution's burden of proof once a customer has notified it of an unauthorized transaction. The aforesaid sub-paragraph places the burden of proof on the financial institution to show that the electronic fund transfer was authorized.

Subparagraph 14 (4) states that the burden of proof in subparagraph (3) shall be satisfied if the financial institution proves that:

- (a) the access code, card and the security of the fund transfer system was fully functional on that day; and
- (b) the officers of or agents appointed by the financial institution were not fraudulent or negligent in carrying out the electronic fund transfer.

⁴⁹ Supra, Benjamin Geva, refer to footnote 36 at p. 81.

Pursuant to the aforesaid paragraphs, if the bank discharges its burden of proof, then this would mean the burden shifts to the customer.

The other instance where the burden shifts to the customer is in the earlier discussed paragraph 15. Professor Benjamin Geva in his commentary on paragraphs 14-19 of BNM/GP 11 has observed that;⁵⁰

“Other than in circumstances in {sic, Paragraph 17(1)(a),(b)} under which the customer is exonerated from liability, when the financial institution meets the burden of proof under either {sic, Paragraph 14(4) or Paragraph 15(1),(2)}, the financial institution is not required to show any causal link between what was proven and the unauthorized transfer with respect to which loss has been incurred. Presumably, however in response to proof by the financial institution under {sic, Paragraph 14(4) or Paragraph 15(1),(2) } , the customer is always free to prove that any of the conditions enumerated in {sic, Paragraph 17(1)} has been met, and thereby release himself or herself from liability. Regardless, there is no definition as to when a transfer is “unauthorized”.”

Professor Benjamin Geva has also noted the anomaly created by the guidelines being silent on any ceiling limit for the customer’s liability in the event the financial institution is able to discharge its burden of proof under Paragraphs 14(4) or 15(1) and (2)- unless the customer totally exonerates liability by virtue of Paragraph 17(1)(a) or(b).⁵¹ The professor elaborates:⁵²

“However, where “the customer has contributed to the loss resulting from an unauthorized transaction by, delaying notification” regarding loss or misuse or theft of the card or breach of code security, liability for actual loss is limited by withdrawal or transactions limits (sic, in the case of credit cards and other forms of electronic funds transfers) as well as account balance (sic, only in the other forms of electronic funds transfer). This introduces ambiguity: it seems unreasonable to read the Guidelines as fastening unlimited liability when the customer contributed to the loss other than by delaying his or her notification, and limited liability when the customer has contributed to the loss by delaying notification. Under {sic, paragraph 17(1)(a)(b)}, the customer is under no liability unless loss has been attributed to or contributed by him or her.”

Overall the BNM/GP 11 Guidelines seem to shift the burden of proof from the financial institutions to the customer with ease. There is evidently no clarity or comprehension from the consumer’s angle given the fact that the consumer is not in a position to defend or proclaim his innocence if the banker alleges that he is privy to the unauthorized transaction. The only supposed right to information accorded to the “accused customer” is stated in paragraph 28 of BNM/GP 11.

⁵⁰ Ibid

⁵¹ Ibid.

⁵² Ibid.

(v) Financial Institution to Provide Information

Paragraph 28 provides: Where a financial institution is of the view that the customer is liable for loss arising from any loss, misuse, theft or unauthorized use of a card or breach of access code security:

- (a) the financial institution is to make available to the customer, copies of any documents or other evidence relevant to the outcome of its investigation, including information from the log of transactions; and
- (b) the financial institution is also to refer to the systems log to establish whether there was any system or equipment malfunction at the time of the transactions, and advise the customer in writing of the outcome of its inquiry.

Provided always that the financial institution will not be required to furnish any information that has direct relation to or impacts the security of the financial institution or its system.

Paragraph 28 is arbitrary as the "financial institution is of the view that the customer is liable" This means the financial institution is the judge and jury in this matter although it is a party to the whole scheme. The writer is of the opinion that this paragraph should be read together with the subsequent Paragraph 29 of the guidelines.

Paragraph 29 Breach of Duties

Where the financial institution, its officers or agents appointed fail to observe the:

- (a) allocation of liability under paragraphs 16 and 17; or
- (b) procedures on complaint, investigation and resolution under paragraphs 25 and 26

and where such a failure prejudiced the outcome of the complaint or resulted in delay in its resolution, the financial institution may be liable for the full amount of the transaction which is the subject of the complaint.

In conclusion, the above stated discussion on BNM/GP 11 providing consumer protection for unauthorized use or transactions has yielded the following observations :

- 1) Firstly, most credit card users are unaware of this guideline; it has been termed as "deadwood" by an officer at Bank Negara. The new PSA 2003 in section 77(4) renders BNM/GP 11 which was issued pursuant to 119(deleted) and 126 BAFIA, as being lawfully issued under section 70 of PSA 2003. BNM/GP 11 has not been amended, rescinded or replaced under the PSA 2003; accordingly the guidelines are still "alive".
- 2) Secondly, the guidelines are not coherent and confusing to the consumer.
- 3) Thirdly, almost all bank officers in the credit card department refer to the Credit Card Guidelines (Version 2.0) as the "Consumer Protection" guideline and not BNM/GP 11. (The Credit Card Guidelines will be discussed next in this paper).
- 4) Lastly, BNM/GP 11 is a concoction for all ailments and therefore a remedy for none. BNM/GP 11 covers all forms of plastic cards although the nature of ATM/Debit cards is different from credit cards. The situation is worsened by the fact it also covers

consumer protection for any other form of electronic funds transfers (excluding PC banking).

(b) Consumer Protection for “unauthorized use” in Credit Card Guidelines (Version 2.0)

(i) The Liability for Lost or Stolen Cards

Paragraph 13 deals specifically with the liability for lost or stolen credit cards. Paragraph 13.1 is similar to Paragraphs 18 and 19 of BNM/GP 11 that imposes on the issuer to provide an effective and convenient method to notify any lost, stolen or unauthorized use of his credit card. The issuers must implement in-house procedures for acknowledging receipt and verification of notification for lost, stolen or unauthorized use of credit card.

Paragraph 13.2 stipulates that :

The cardholder’s maximum liability for unauthorized transactions as a consequence of a lost or stolen credit card shall be confined to a limit specified by the issuer of credit cards, which shall not exceed RM250.

There are two provisos to this paragraph, namely :

- (a) The cardholder has not acted fraudulently; or
- (b) The cardholder has not failed to inform the issuer of the credit cards as soon reasonably practicable after having found that his credit card is lost or stolen.

Therefore the guidelines do impose a ceiling of liability for a bona fide consumer caught in an unauthorized transaction. At this juncture, it is noted that these guidelines do not define the terminology “unauthorized”.

Paragraph 13.3 permits the issuer to exceed the RM250 mark if it can prove either one of the above stated two provisos. Pursuant to paragraph 13.5, this imposition of liability is notified to the cardholder in his monthly billing statement. However, it is noted that the degree of action in both the provisos differ; the first proviso deals with a criminal intent namely fraud but the second proviso is merely carelessness or negligence of the consumer in delaying or not notifying the issuer. Since both the actions greatly differ in nature it is rather harsh not to impose any limitation for at least the second proviso. It is suggested that if the consumer has not grossly delayed notification, then it is fair to impose liability until the credit limit of his card.

{This is stipulated in the earlier discussed BNM/GP 11, paragraph 16(a)}. In this context, there appears to be a conflict between these guidelines and BNM/GP11.

Lastly, paragraph 13.4 ensures that the cardholder is not liable for any unauthorized transaction charged to the credit card after notification either verbally or in writing. These guidelines (unlike BNM/GP 11) do expressly allow oral notification. Immediately upon notification, the issuer shall take action to prevent further use of the lost or stolen card.

In conclusion,

- 1) The Credit Card Guidelines (Version 2.0) is the guideline being currently and actively implemented by financial institutions.
- 2) The aforesaid guideline is in essence a non consumer protection guideline although it does contain some protection to the user-it is more a regulatory guideline for providing a standard and efficient credit card scheme.
- 3) The guidelines do contain a penalty, whereby pursuant to paragraph 1.1, non compliance with the guidelines is an offence punishable under section 57 PSA 2003. (A hefty fine of RM500, 000 and an extra RM1,000 for every day the offence continues!)
- 4) There is conflict between BNM/GP 11 drafted in 1998 and the Credit Card Guidelines issued in 2004. Which is to prevail?....The banker says the Credit Card Guidelines (Version 2.0) but then again it is not a consumer protection guideline.

5. The Code of Good Banking Practice

The 'Code of Good Banking Practice' was issued by the Association of Banks in Malaysia (ABM) in 1995. The Code sets out the manner banks are required to deal with their customers in areas such as account opening, charges and interest rates, complaints and disputes confidentiality, marketing of services etc.⁵³ The Code is the banking industry standard implemented by ABM to implement 'good' or positive banking practices. In relation to credit cards, the Code requires banks to inform customers about their responsibilities of safeguarding their cards and PINs to prevent fraud. Customers should be clearly informed of their liabilities and the bank's liabilities in the event of unauthorized use or transactions using their credit cards.⁵⁴

6. The Financial Mediation Bureau.

Both the BNM/GP 11 and the Credit Card Guidelines (Version 2.0) stipulate that the bank provide an 'in - house' procedure to resolve any dispute relating to the unauthorized use of credit cards. If the consumer is unhappy with the 'in - house' decision of the bank, he can lodge a complaint with the Financial Mediation Bureau. The Financial Mediation Bureau deals with claims relating to credit card fraud up to a limit of RM25, 000. The customer has to exhaust the avenue provided by the bank first before resorting to the mediation process. Therefore the customer has to hand to the mediation bureau a 'final decision' letter from the bank indicating the matter has not been resolved. Then the customer has to complete and submit to the mediation bureau a Complaints Form and a Consent Form to permit the banker to disclose to the mediator all information relation to his account.⁵⁵ This mediation bureau acts as a 'middle person' to resolve any conflict between the parties. If the customer is still unhappy with the mediation bureau's decision, he can then refer the matter to a court of law. Therefore, the courts will be the final destination of a disgruntled customer.

⁵³ See article "Promoting Good Banking Practice". <http://abm.org.my> (accessed on 27/9/07)

⁵⁴ Ibid.

⁵⁵ This is an exception to the banker's duty of secrecy provided by sec 99(a) BAFIA.

7. Consumer Protection Statutes In Other Jurisdictions

7.1 United Kingdom

(a) The Consumer Credit Act 1974

The UK Consumer Credit Act 1974 covers credit card agreements as it falls within the definition of “credit token agreements” in section 14 of the aforesaid Act. Section 14 of the UK Consumer Credit Act states that :

- (1) A credit token is a card, check, voucher, coupon, stamp, form, booklet or other document or thing given to an individual by a person carrying on a consumer credit business, who undertakes-
 - (a) that on production of it (whether or not some other action is also required) he will supply cash, goods and services (or any of them) on credit, or
 - (b) that where, on production of it to a third party (whether or not any other action is also required), the third party supplies cash, goods and services (or any of them), he will pay the third party for them (whether or not deducting any discount or commission), in return for payment to him by the individual.
- (2) A credit token agreement is a regulated agreement for the provision of credit in connection with the use of a credit token.
- (3) Without prejudice to the generality of section 9(1), the person who gives to an individual an undertaking falling within subsection 1(b) shall be taken to provide him with credit drawn on whenever a third party supplies him with cash, goods or services.
- (4) For the purposes of subsection (1), use of an object to operate a machine provided by the person giving the object or a third party shall be treated as production of the object to him.

The above stated definition of “credit token” in section 14 subsections (1) and (4) is in *pari materia* with the definition of “credit token” in BAFIA 1989 prior to the amendments in 2003. The Malaysian definition of “credit token” was deleted in 2003 by Act A1211. Therefore the term “credit token” has ceased to exist in Malaysia.

The UK Consumer Credit Act 1974 contains several protections for credit card users; the writer will concentrate on section relating to unauthorized use of the credit card. The two relevant sections are Section 83 and Section 84 of the said Act. Section 83 states that a “debtor shall not be liable to the creditor for any loss arising from the use of the **credit facility** by another person not acting, or to be treated as acting, as the debtor’s agent.” This is to be read together with Section 173(1) which renders void any term of a credit card agreement that is contrary to this protection.⁵⁶ If the debtor states that a rogue was not acting, nor was to be

⁵⁶ Refer to Consumer Liability for credit card fraud, Paul Stokes, 155 New Law Journal 1342.

treated as acting, as his agent in using the card, then Section 171(4) places the onus of proof on the creditor to prove the contrary.⁵⁷

However the application of Section 83 to credit cards has to be read in light of Section 84 that does impose a minimal liability. Section 84 of the UK Consumer Credit Act 1974 titled "Misuse of credit tokens" deals with liability of a debtor whose credit token ceases to be in his possession and is used by any person not authorized by the debtor. Pursuant to the said section 84 Subsection (1) and (3), the debtor is only liable up to the limit of £50 (or the credit limit if lower) for fraudulent transactions that occur before the creditor is officially notified of the loss.

The notification for 'misuse' and either be oral or written but if it is in the oral form and the credit token agreement so requires, then it must be re-confirmed in writing within seven days.⁵⁸ Section 84 (2) states that a debtor can be liable for losses if the person who misused the credit card obtained it with the debtor's consent. In order for the consent to be effective, it must not have been obtained by force, subterfuge or coercion.⁵⁹ The limited liability imposed by Section 84(1) and the unlimited liability imposed by Section 84(2) is dependant on the requirement that the credit token agreement must set out details of a person or body to be contacted in the event of loss or theft of the card. This section also provides that any sum paid by the cardholder for the issuing of the card is to be treated as paid towards his liability for loss unless it has been previously set off against amounts due for the use of the token.⁶⁰ In addition, if more than one token is issued under one agreement, the applicable provisions apply to each token separately.⁶¹ This means that each supplementary card has also has a ceiling liability of £50 for misuse prior to any official notification to the bank.

Ellinger's Modern Banking Law has made some salient observations on the scope of this section.⁶² The learned author states as follows:

"The cardholder's liability under section 84 is confined to cases in which the agreement between the parties includes appropriate clauses. If the agreement is silent, the position is governed by the general provisions of section 83, which frees the cardholder from liability for loss in the case of misuse. But the section is subject to one important limitation. It applies only to unauthorized use of the 'credit facility'. It has accordingly been argued that if 'the debtor maintains an account with the creditor and there is a credit balance on the account in favour of the debtor, nothing in section 83 would prevent the debtor being made liable to the creditor for any loss arising from the unauthorized withdrawals of that credit balance."

Nevertheless, Ellinger concedes that the above proposition should also take into account the UK Banking Code that imposes a limit of £50 in the event of misuse of a card before notification of its loss.⁶³

⁵⁷ Ibid.

⁵⁸ Section 84(3) and (5) UK Consumer Credit Act 1974.

⁵⁹ *Supra*, footnote 55.

⁶⁰ Section 84(6)

⁶¹ Section 84(8)

⁶² Ellinger's Modern Banking Law, E.P.Ellinger, E.Lomnicka,R.J.A. Hooley, Fourth edition, Oxford University Press at p 604.

The UK Consumer Credit Act 1974 has been in existence for the past 30 years and was primarily designed to protect the consumers. Therefore unlike our Credit Card Guidelines Version 2.0, it offers more comprehensive protection to the consumers. Recently the 1974 Act was revised by the UK Consumer Credit Act 2006 which updates further the legal protection granted to consumers.

The protection afforded to credit holders in UK is further strengthened by two EU Directives known as "distance marketing" Directives.⁶⁴ Section 84 does not apply when a credit token is used to effect 'distance contracts' which are contracts concluded over the internet, email or telephone. (Contracts where the customers are not physically present to conduct the transaction). Therefore fraudulent use of payment cards for 'distance contracts' are cancelable and the customer is entitled to have his account re-credited.⁶⁵ In such circumstances the general principles in Section 83 will apply.⁶⁶

7.2 Consumer Protection in the United States

(a) The Truth-In-Lending Act (4th ed. And Supp)

The Truth-In-Lending Act and its regulations, Regulation Z applies to credit card transactions. Regulation Z defines a credit card as any card, plate, coupon, book or other single credit device that may be used from time to time to obtain credit.⁶⁷ Budnitz and Saunders explain the extent of liability of a credit card holder as follows:⁶⁸

"TILA (Truth-In Lending Act) limits the cardholder's liability for unauthorized use of a credit card. The cardholder is not liable in any amount for unauthorized use unless the card comes within the definition of an "accepted card"⁶⁹, the card issuer has provided the customer with notice of the limits of liability for unauthorized use, and the issuer has provided a means to identify the cardholder or the authorized user of the account. If the card issuer has complied with the above requirements, the consumer is liable up to a maximum of the lesser fifty dollars "or the amount of money, property, labor, or services obtained by the unauthorized use before notification to the card issuer as required by Regulation Z."

Overall, an examination of Regulation Z indicates a more comprehensive and specifically designed statute governing unauthorized use of the credit card in comparison to the 'confusing' structure in Malaysia. The reason being, Regulation Z was designed primarily to deal with consumer protection issues.

⁶³ Ibid.
⁶⁴ Refer to Section 84 (3A)-(3D) UK Consumer Credit Act 1974 and added by Consumer Protection (Distance Selling) Regulations 2001, S.I. 2001/2334 and the Financial Services (Distance Marketing) Regulations 2004, S.I. 2004/2095.
⁶⁵ Supra Ellinger at footnote 61, at p 605.
⁶⁶ Ibid.
⁶⁷ 12 C.F.R. § 226.2(15).
⁶⁸ Supra footnote 30 at p 57
⁶⁹ A credit card "that a cardholder has requested or applied for and received, or has signed, used or authorized another person to use to obtain credit", Reg Z, 12 C.F.R. § 226.12(b)(2)(i), Note 21.

Conclusion

Several years ago, the bankers in Malaysia initiated a campaign named "Make the Switch" to promote the use of electronic banking and electronic devices. The move not only in Malaysia, but throughout the world is to shift to a 'cashless' society. The credit card is the most favourite device actively used by consumers, mainly the younger generation who wish to avoid being burdened by heavy wallets as well as the danger of being mugged. The writer feels that the current banking consumer protection legislation in Malaysia is inadequate and not comprehensive enough to deal with the pitfalls of using a credit card especially in cases of fraudulent use. It would be in the best interest of the banking fraternity to balance profits generated by the credit cards with the rights of the banking consumer. At the end of the day, the consumer has to be assured that in time of a crisis; he has an avenue to seek redress in a legal system which is uncomplicated, simple and easy to comprehend.

