An Investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China

by

Yan Sun

Doctoral Thesis

Submitted in partial fulfilment of the requirements

for the award of

Doctor of Philosophy of Loughborough University

May 2010

Loughborough University

CERTIFICATE OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this thesis, that the original work is my own except as specified in acknowledgments or in footnotes, and that neither the thesis nor the original work contained therein has been submitted to this or any other institution for a degree.

…… (Signed)

…… (Date)

Acknowledgement

I believe that the experience of doing a PhD is unique for each candidate. For me, the achievement is more than a degree but represents the bitter-sweet journey of being independent in the UK, which is 5,634 miles away from my hometown, Xi'an, China.

Firstly, I would love to express my endless gratitude to Professor Ian R Davidson, my supervisor, who has been helping me all the way along to achieve my PhD degree. This thesis and research project would not have been possible without his professional guidance and consistent encouragement at each stage. His comments and advice are always inspiring when I face unexpected challenges in my study. His lovely family, Judy, Iona, Jazz and Shadow are parts of the support team who welcome me sincerely and make me feel at home in the UK.

Mostly, I must say one million thanks to my big sweet family in China, in particular to my parents Yong and Xiaoli. They are the best parents in the world that I can ever wish for, and they never have any doubt on me even when I lost faith in myself. Their patience and love help me find my way back on the right track when I got lost. My loving grandma, Jizhen Huang, is an extraordinary lady, with whom I spent my whole childhood and started to learn this world from an interesting aspect. Last but not the least, I own a big thank you to my personal IT support, Dr. Xing Zhang, who has been by my side throughout my PhD study and working very hard to deal with all kinds of IT problems I came across.

Additional academic support from members of the Business School and Loughborough University is gratefully acknowledged. In particular Prof. Barry Howcraft, Prof. Neil Dorherty and Dr. Baibing Li have provided valuable feedback on my project.

Also, special thanks must go to the industry contacts and survey respondents from both the UK and China.

The financial support provided by Loughborough University and Business School is gratefully acknowledged.

Dedication

This doctoral thesis is dedicated to my late grandfather, Dr. Shaoliang Sun, an outstanding surgeon in China who had devoted his whole life saving lives and rescuing souls. I miss you so much, grandpa, and I love you forever.

Abstract

This doctoral thesis represents an investigation into financial fraud in online banking and card payment systems in the UK and China, involving network security, online financial transactions, internet fraud, card payment systems and individuals' perception of and behaviours towards electronic environments. In contrast to previous studies, the research questions were tackled by survey questionnaires both in the UK and China, with a particular interest in fraud and attempted fraud.

The main findings from the UK respondents were that those with higher IT skill and younger respondents are more likely to be defrauded on the internet. Certain types of online activities are associated with higher risks of fraud, these being internet banking; online shopping and media downloading. Furthermore, four predictors (internet banking, online education services, downloading media and length of debit card usage) provided significant effects in the logistic regression model to explain fraud occurrence in the UK.

Based on the data collected in China, younger respondents were more likely to have higher general IT skill and higher educational qualifications. However, online shopping was the only online activity which was significantly correlated to fraud occurrence. Finally, two predictors (frequency of usage of online shopping and number of debit cards) were selected in the logistic regression model to explain fraud occurrence in China.

Key words:

Financial transactions, internet fraud, online payment, credit card, debit card, network security, internet banking, online shopping, customers' satisfaction, cyber crimes.

Content

List of Tables

List of Figures

Glossary of Terms

APACS	UK Payments Administration
AVC	Address Verification Check
AVS/CSC	Address Verification System / Card Security Code
BASE II	Data processing network operated by Visa Usa for clearing and settlement of bank card transactions
CAVV	Cardholder Authentication Verification Value
CCJ	County Court Judgments
CERN	the European Organization for Nuclear Research
CNCERT / CC	National Computer Network Emergency Response Technical Team / Coordination Center of China
CNNIC	China Internet Network Information Center
CNP	Card-not-present
CVV2	Card Verification Value
ECI	Electronic Commerce Indicator
EMV	a standard for interoperation of integrated circuit cards (IC cards or "chip cards") and IC card capable POS terminals and ATMs, for authenticating credit and debit card transactions. EMV comes from the initial letters of Europay, MasterCard and VISA
HTTP	Hypertext Transfer Protocol
HUDC	History Of Debit Card Usage
IC3	The Internet Crime Complaint Center
IP	Internet Protocol
ISS	Internet Security System
LDAP	the Lightweight Directory Access Protocol
LDV	Limited Dependent Variable
NW3C	National White Collar Crime Center
PCT	Private Communications Technology
PIN	Personal Identification Number
POP3	the Post Office Protocol
POS	Point of Sale

SMS	Short Message Service
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UCE	Unsolicited Commercial Email
UDDI	Universal Description, Discovery and Integration
UOOADM	Usage Of Online Downloading Media
UOOAOES	Usage Of Online Education Service
VIP	Visa Integrated Payment Platform
Wi-Fi	Wi-Fi Alliance
WSDL	Web Service Definition Language
WSFL	Web Services Flow Language
XIO	a packet-based, high-performance computer bus protocol
XML	Extensible Markup Language

Chapter 1 Introduction

1.1 Introduction

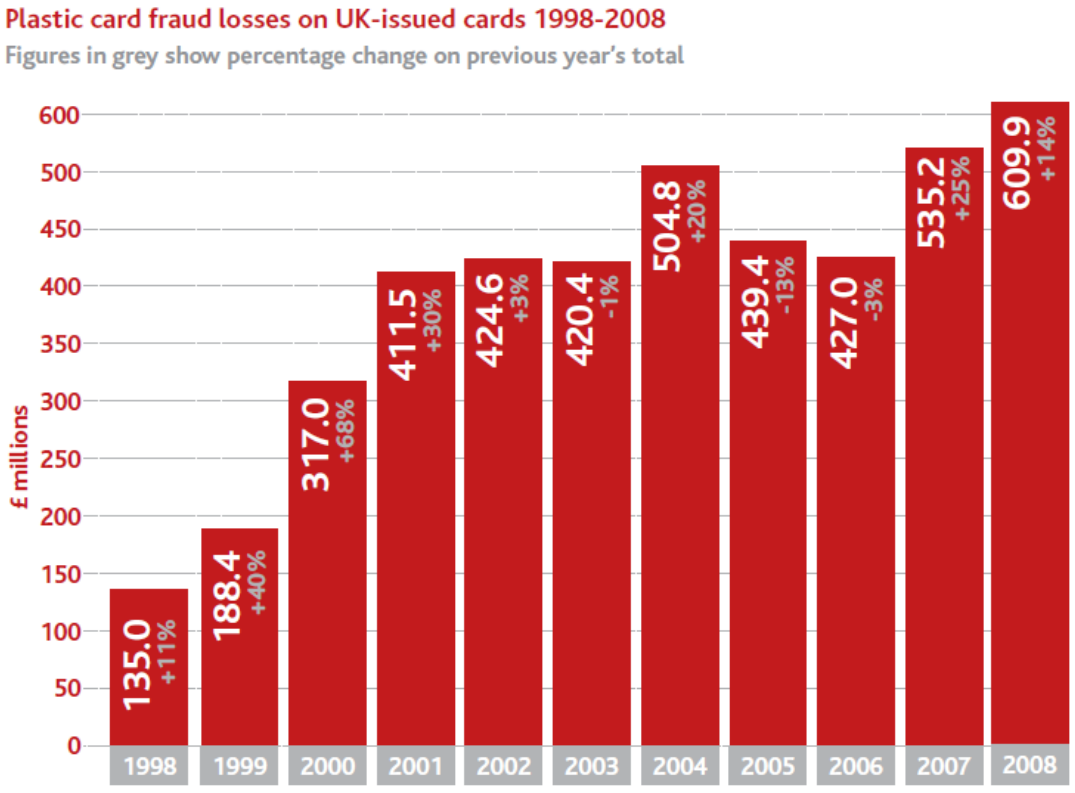
This chapter is the introduction to the thesis 'an investigation of financial fraud in online banking and card payment systems in the UK and China'. In this introductory chapter, we address the key questions of interest, explain why they are important, provide a roadmap of the structure of the dissertation and give a brief overview of the main conclusions.

1.2 How secure are electronic transactions systems and how secure do people perceive them to be?

Electronic transactions systems designed for use by customers / consumers cover a variety of channels including point of sale (POS), internet banking, internet credit card payments and even settlements partially involving telephone instructions such as 'card-not-present' payments. There are two key sides to the problem. On the one hand, we are interested in how secure these systems are from a technical point of view – ie how do these systems operate? What are their vulnerabilities, and how are these exploited? On the other hand, there is the question of consumer confidence – ie how happy are customers / consumers to use the systems, given that they do not understand them other than superficially, even though they might be quite adept at operating them? A third question, which we reflect on in the conclusions, is how sustainable are some of these transactions systems? Who will win the battle for control? Will the fraudsters eventually make some of the media, such as the internet, unsafe and unusable for financial transactions, or will the systems experts in the banks and credit card companies eliminate electronic fraud? Alternatively, will there continue to be an uneasy equilibrium with the balance swinging between the fraudsters on one occasion and the systems experts on the other? This last scenario may even be the best outcome

for fraudsters, because if they eradicate the internet as a medium for financial transactions, they will remove their means of exploiting it.

According to a popular article in the Sunday Express (Abbott 23/08/2009, p7), more than one in 10 of Britain's 20 million online shoppers has either parted with money on a bogus website or knows someone who has. Although this is not to be regarded as a rigorous scientific study, the general message is consistent with the survey data we collected in the UK, where about 21% of the respondents had experienced internet fraud involving various types of online financial transaction. According to the latest survey conducted in 2009 by APACS, the UK Payment Association, the fraud losses involving the internet and bank cards have kept increasing in the last three years (Fraud the facts, 2009), and as the diagram below shows, the loss in the UK alone reached £609.9 million pounds in 2008. This is clearly a very serious problem, and one which we try to analyse in this thesis.



(source: (APACS 2009))
Figure 1.1 Plastic card losses on UK-issued cards 1998-2008

1.3 Overview of previous research

Some of the previous studies of online transactions have focused on the customers' general behaviours and attitudes from a marketing research perspective, for example, individuals' responses to innovations in IT; customers' adoption of online shopping and acceptance of internet banking. Many studies were trying to explain the difference between individuals who accept online services such as internet shopping, e-banking etc and those who reject them, primarily to assist with marketing strategy and building customers' relationships. Particular aspects of interest were:

(a) factual investigations into individuals' usage of e-transactions, and

(b) internet demographics and psychology, as a logical extension of the findings in (a), to provide understanding of the slow adoption of online financial transaction media such as e-banking. For example, Howcroft, *et al,* (2002) studied demographic characteristics of respondents including gender, age, annual income, level of education and ownership of financial products. As a by-product of this line of enquiry, researchers were trying to develop strategies that would attract customers to online products and services.

Another line of research into online financial transaction systems has involved detailed analysis of the computer science and IT technology in areas such as network construction, internet protocols and data security. This area is complex and only fully understood by specialists who are expert in computer science. Nevertheless, this is an important part of the picture and in chapter 2 there is a discussion of the data transmission protocols, network security and the systems that embody these to provide an overall picture of technical aspects of electronic transactions systems and their weaknesses. The core literatures in this area deal with:

(a) the characteristics of the internet and data transmission introducing the basic characteristics of the internet including publicity, anonymity, diversity, non-geographical limitation, digitalized environment etc (Tzenga *et al.* 2005), together with the process of data transmission on the internet using SSL protocol (Onyszko 2006).

(b) different schemes of fraud on the internet, as defined by the Criminal Division,U.S. Department of Justice, and

(c) attacks from the internet, such as those listed by Whitman and Mattord (2003) who addressed fifteen types of attacks used to compromise information systems.

The literature on online transactions combines elements of both the aspects described above – ie customer facing issues and the technicalities as described above – as these are both essential ingredients of the whole picture. This literature goes on to look at some of the broader issues, and can be divided into various themes as follows:
(a) the framework of the online financial transaction explained using the diagrams of transaction flow by Visa -(VISA) Visa: process diagrams (2006);
(b) fraudulent schemes targeting bank cards such as those shown by figures, tables and diagrams from APACS (2006; 2007).
(c) internet crime worldwide including black market transactions on the internet, as illustrated by Greenemier, L. and Hoover, N. (12 Feb 2007) and IC3 2006 Internet Crime Report in USA (2006) and Hong Kong 2006 findings (KPMG HK 2006).

It is this latter area that is the main focus of this thesis. A major gap in the literature is individuals' attitudes to fraud, and also investigation of the factors which might make them vulnerable to fraud. Individuals who have experienced real fraud have had little attention in the literature and have not been studied in detail. One of the main purposes of this dissertation is to help to fill this gap, and surveys in the UK and China were undertaken for this purpose. The UK was chosen on the basis of being a mature 'western' style economy; China on the basis of being the largest of the emergent economies. These countries have both similarities and significant differences in their legal systems as applied to electronic transactions, particularly in relation to the consequences of fraud, as explored in chapter 3. The differences have consequences for the degree of customer satisfaction with the response to fraud as found when comparing the survey data for the two countries in chapter 9.

1.4 Overview of the structure of the dissertation

There are ten chapters in this thesis: Chapter 1 introduces the research questions, the importance of the study, the gaps in the literature that the thesis attempts to fill, and an

overview of the whole thesis; Chapter 2, 3 and 4 contain a review of the relevant literature, with chapter 2 concentrating on the technicalities of electronic transactions and the systems in which they are embedded, chapter 3 discussing the legal environments of the US, UK, EU and China. Chapter 4 is concerned with the literature that relates to the customer's use of the various electronic transaction media and the activities and impact of fraudsters. Chapter 5 discusses the possibilities of different research methods that could be applied to my study and explains the approaches used for data collection and analysis. Chapter 6 details the processes of the data collection and statistical analysis of the data collected in the UK; Chapter 7 introduces the development of the banking system and financial industry in China, covering financial policy, market environment, the characteristics of customers, society culture and other topics; Chapter 8 addresses the field work, including the sample selection and data collection in China and the results obtained; Chapter 9 compares the findings from the UK and China, using statistical testing to investigate the significance of the differences found; Chapter 10 contains the conclusions, summarizing the findings of this study and providing ideas about future directions of research.

1.5 Conclusion

The findings of this thesis are presented in the concluding chapter together with reflections on the future research and the sustainability of the various forms of financial transaction. In terms of the surveys, there were reassuring consistencies between the findings in the UK and in China. However, there were also some key differences – such as the lower incidence of actual fraud in China data but also the lower level of satisfaction with the banks handling of the situation when fraud did occur. Are electronic transactions systems sustainable into the future? It is an open question, with some procedures more vulnerable than others. A discussion of this is provided in the concluding chapter.

The main findings from the survey questionnaires conducted in the UK and China were that younger respondents are more likely to have higher general IT skill;

respondents with higher IT skill are more likely to be defrauded on the internet; respondents with higher qualifications are more likely to have higher IT skill; younger respondents are more likely to be defrauded on the internet. Also, certain types of online activities are associated with higher risks of fraud, particularly online shopping and media downloading (but not online gaming). Furthermore, four predictors (usage of internet banking, usage of online education services, and usage of downloading media and length of debit card usage) provided significant effects in the logistic regression model to predict fraud occurrence in the UK.

Based on the data collected in China, we found that younger respondents are more likely to have higher general IT skill; respondents with higher qualification are more likely to have higher IT skill. However, online shopping was discovered as the only online activity which was significantly correlated with fraud occurrence. Finally, two predictors (frequency of usage of online shopping and number of debit cards) provided significant effects in the logistic regression model to predict fraud occurrence in China.

Chapter 2 Security and Fraud in Electronic and Online Environment

2.1 Introduction

The purpose of this chapter is to provide a discussion of the way that electronic and internet security systems are set up and the vulnerabilities that they are subject to. This is crucial to understanding the environment in which electronic financial transactions take place and the problems that are faced in combating fraudsters who are becoming increasingly sophisticated. The following chapter extends this discussion into the legal environment surrounding online and automated financial transactions by looking at the financial flows involved in online transactions and card payments.

2.2 Network technology and security

2.2.1 Evolution of the Internet

In contrast to the physical world which has lots of unchangeable limits, the internet is an open space, which offers greater freedom for people to communicate. The internet was developed mainly in the US in the 1970s using the new technique of 'packet switching' (a term coined by British Scientist Donald Davis) and it was still unknown to the general public in 1990 (Baker 2002/2). At the end of 1990, a revolution took place in CERN, the European Organization for Nuclear Research, where another British scientist, Tim Berners-Lee, combined the internet's Transmission Control Protocol (TCP) with hypertext and created the world's first-ever web site (CERN). The objective was to create a single information network to help CERN physicists share all the computer-stored information at the laboratory (CERN).

By the year 2000, the internet had millions of users throughout the world (Baker 2002/2). According to the figures from the CIA in 2005, there were 37.6 million people who used the internet in the UK alone (CIA 2005). For many people the internet has become part of their daily life. We depend on the internet more and more not only to contact family, friends and colleagues, but also to search and exchange all

kinds of information without geographic limitation, subject only to comprehension of the language or graphic indicators used. As most websites are written in English, the internet has become one of the most important drivers for the adoption of English as an international language.

First of all, we look at the characteristics of internet including its strengths and weaknesses, advantages and disadvantages particularly with financial transactions in mind. The characteristics of the internet are shown as below (Tzenga *et al.* 2005):

(1) Publicity: over the internet, there is no need to know a users' identity, location or application programmes. Each user can send or receive data or information through the internet.

(2) Anonymity: we may occasionally obtain the user's IP address while sending or receiving data, but we are unable to get other information about the user, unless some special approaches are taken.

(3) Diversity: anyone can, in any form, develop or do anything because the internet is public so that the information contained in the internet is quite diverse.

(4) Non-geographical limitation: internet users come from all over the world without being affected by geographical differences and are able to communicate with one another from anywhere at anytime.

(5) Digitalized environment: any information transfer over the internet is by means of a digital file, so obtaining or copying or it is a straightforward task encryption coding might be required to read it.

As a medium the internet lets people communicate to each other in a real time with low cost and high efficiency. The sheer diversity of information makes the internet the richest source for any information available. The digitalized environment creates a virtual space for internet users and inspires people's imagination without limits. Unfortunately, while people are overwhelmed by the advantages and possibilities of the internet, it is not without problems as a medium for both social interactions and financial transactions.

The internet was designed for openness and simplicity (Gralla 2006,p9). That is to say that online information is supposed to be sent back and forth easily and totally open to

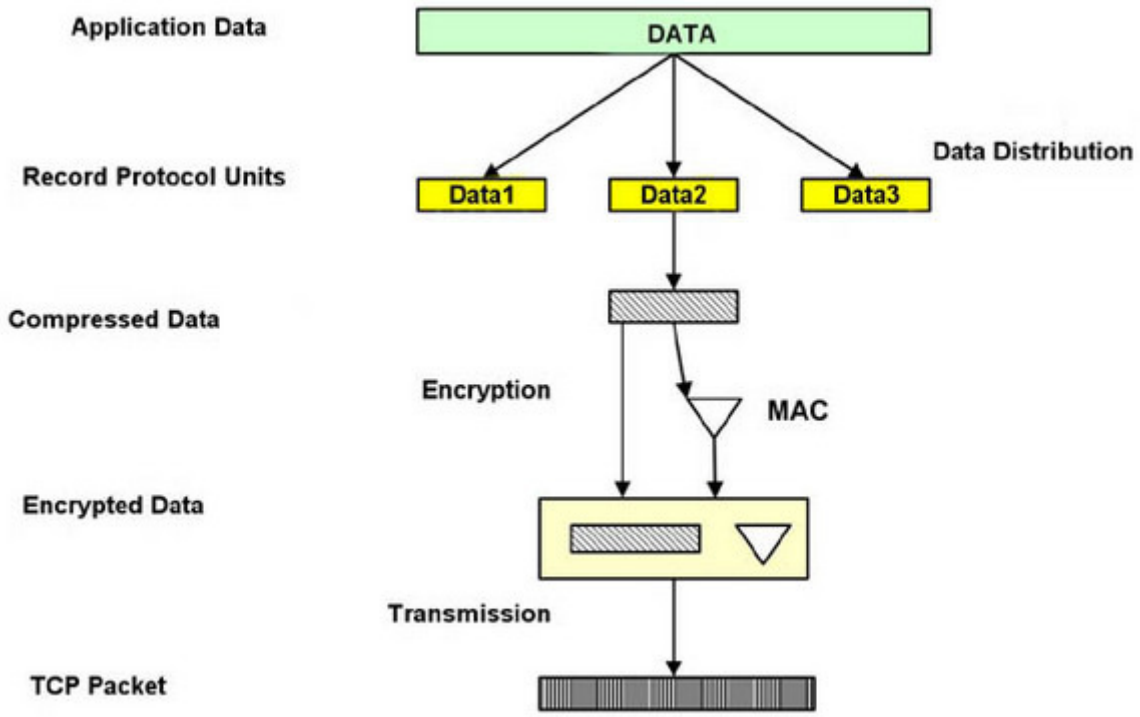
anyone. Anyone who knows a little technical knowledge can take advantage of the internet for his own purpose and this could involve criminal activity. In contrast to more traditional channels of communication, the internet makes it easy for anyone to hide his true identity or even pose as someone else (Gralla 2006,p9). For example, it is very common and easy to register an e-mail account using fake personal information, such as name, gender, age, address etc. As opposed to a postal address, an email address is only a virtual code for one user and it doesn't necessarily convey any clue of physical existence or identification. You can't be sure who a person is from their email addresses, nor where they come from, nor can you be sure if this is the same person you contacted minutes before. In the cyber world, neither identification nor location can be determined with certainty.

2.2.2 Data transmission on the internet (general protocols)

The security of data transmission on the internet becomes more and more important because of the rapid growth of internet users using the medium for business and financial transactions as well as more general communications. For financial services in particular, security on the internet becomes the key factor for each party involved in the online transaction.

On the internet, data transmission not only relies on the hardware connection, but also depends on the various protocols for data transmission, such as TCP/IP, SSL etc. In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. These protocols break up every piece of information and message into pieces called packets, deliver those packets to the coded destinations, and then reassemble the packets into their original form after they have been delivered so the receiving computer can view and use them (Gralla 2006,p9). TCP is the Transmission Control Protocol and IP is the Internet Protocol. TCP breaks up information into packets and reassembles the packets at the receivers' end. IP is responsible for ensuring the packets are sent to the right destination (Gralla 2006,p9).

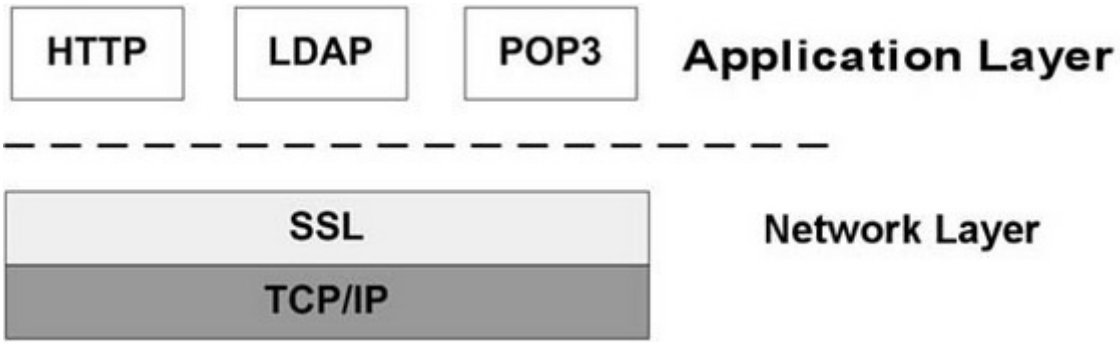
Figure 2.1 shows the process of the preparation of data to be sent on the internet. The application data in this diagram refers to a message to be transmitted to another user. The content of this message consists of data, which are first divided into Record Protocol Units. These are then compressed and encrypted, using the public key to encrypt the data in order to ensure secure transmission on the internet. The original message is now in the form of a series of packets, which are ready for secure transmission. When these packets reach the client terminal, they are decrypted to the original message by using the private key which is offered by the server. The main function of SSL (Secure Socket Layer) is authenticating the client and server to each other; ensuring data integrity and securing data privacy (Onyszko 2006).



(source: (Onyszko 2006))

Figure 2.1 Creating a packet under SSL record protocol

"The SSL protocol was originally developed by Netscape, to ensure security of data transported and routed through HTTP, LDAP or POP3 application layers. SSL is designed to make use of TCP as a communication layer to provide a reliable end-to-end secure and authenticated connection between two points over a network (for example between the service client and the server)" (Onyszko 2006). TCP/IP is the basic protocol for data transmission on the internet. SSL is the senior protocol which supports the use of standard key encryption technologies. This is illustrated diagrammatically in Figure 2.2 below:



(source: (Onyszko 2006))

Figure 2.2 SSL between application protocols and TCP/IP

Hagel and Brown (2001) on the other hand divide the web service into three layers consisting of the application service layer, the service grid layer, and the standards and protocols layer. Ratnasingam (2002) summarised the characteristics of the three layers as follows:

1. *Top layer – application service*. Web services run on any application platform as long as it has a web server connected to the internet.
2. *Middle layer – service grid*. The service grid layer provides four types of utilities:

- service management utilities (including provisioning, monitoring, ensuring quality of service, synchronization and conflict resolution);
- resource knowledge management utilities (including directories, brokers, registries, repositories and data transformation);

- transport management utilities (including message queuing, filtering, metering, monitoring, routing and resource orchestration); and
- shared utilities (including security, auditing and assessment of third party performance, billing and payment).

3. *Bottom layer – software standards and communication protocols*. Software standards include:

- WSDL to describe the Web service;
- UDDI to advertise, syndicate as a central organization for registering, finding and using Web services;
- Web services flow language (WSFL) to define work flows;
- XML to format data exchange and description; and
- Communication protocols (including SOAP to communicate that is for calling Web services, HTTP and TCP/IP).

In security terms, it is apparent from the explanations above that the bottom layer is fundamental in that it deals with basic coded security such as SSL, whereas the middle layer contains security software such as firewalls which is subject to change and development. Both layers have susceptibilities to security problems.

2.2.3 Vulnerabilities of protocols

SSL seemed good enough to ensure that data transmission online was safe from a technical perspective. But in practice, its vulnerability affects tens of thousands of sites. In 2004, the researchers of Netcraft (Bekker 2004) noted that the key vulnerability of SSL is stack overflow in the Private Communications Technology, or PCT, protocol. PCT is a proprietary protocol developed by Microsoft and Visa International as an alternative to Secure Sockets Layer (SSL) 2.0. SSL 3.0 has made obsolete both PCT 1.0 and SSL 2.0. PCT is enabled by default in Windows 2000 and Windows NT 4.0. Windows Server 2003 has SSL 3.0 enabled and PCT disabled by default.

Although Microsoft keeps releasing new patches in order to fix the security problems, many customers will not be patched for weeks or months. According to the March Secure Server Survey by Netcraft in 2004 (Bekker 2004), more than 132,000 web-facing SSL servers were running either Windows 2000 or Windows NT4. When the network researchers are still in the discussion of vulnerability of SSL, the criminals already have started to try new fraud schemes on the internet with more advanced tricks. The X-Force security researchers at Internet Security System (ISS) stated: "the SSL is so often used for secure data transmissions involving confidential or financial information that hackers will aggressively target any vulnerability given the high-value nature of websites protected by SSL" (Bekker 2004).

When Microsoft fixed two remote code execution vulnerabilities in Powerpoint, researchers mentioned that this flaw is particularly dangerous because it doesn't require any user interaction and could allow an attacker to gain complete control over the targeted system, giving them the ability to alter or delete data and create new user accounts with full privileges (Espiner 2009).

When people realize the importance of internet security they are normally willing to have an SSL connection to encrypt all information flows with the internet. Even unsophisticated users are learning never to click on links or attachments in unfamiliar emails because of the increased publicity given to internet security in the general media (kranky 2006). While customers seek protection from up-to-date software and new protocols, cyber criminals also look for the vulnerabilities and weakness of internet security systems. As phishing emails become less effective, cyber criminals are turning to a relatively new and frightening method, so called SSL-evading Trojans (kranky 2006). The real danger of these Trojans is that they don't break the encryption at all which means the encryption connection remains complete while the fraudsters enter the user's accounts.

These Trojans are using three main methods: the first one is called "Bogus SSL", which can find financial websites in the browser cache and create fake local pages (kranky 2006). When users try to log on to the real website, the Trojans divert users to the fake webpage and capture their logon information. Then users will be diverted back to the real website and therefore users don't notice anything wrong.

The second method is called “password-grabbing scheme”. When financial websites want to identify the online users, they usually show some graphics and random numbers on the webpage and ask users to enter these. In this situation, the Trojans can take snapshots of the part of the screen and send them back to the hacker (kranky 2006).

The third method that Trojans can use is to bypass any existing authentication after a users’ PC has been infected. Once the Trojans are on a user’s machine, they can wait for any chance patiently. When the users log in to their online accounts successfully, the Trojans can initiate payments or transfers to anywhere by creating hidden browser windows to make transactions (kranky 2006). This fraud is very difficult for financial websites to detect because the transaction is being done from an authorized user using successfully logged on websites.

Defenses against intrusions need to be in place and to be updated constantly. Internet experts and internet criminals continuously compete against each other but at the same time they inspire and encourage each other. To a large extent, the development of internet security technology is the outcome of a secret war between two totally opposite powers.

2.2.4 Encryption and decryption

Given the importance of data encryption for preserving the security of online communications and transactions, it is appropriate at this point to outline the mechanisms and techniques for data encryption and to assess their rôle particularly in guarding against fraud.

2.2.4.1 Secret key encryption;

Secret key encryption, also known as symmetric cryptography, uses a single key for both encryption and decryption. In the following diagrams we can see the process of message sending from A to B. After the encryption, A sends out the message. On the other side, B only gets the correct message from A if B decrypts the message

successfully. This symmetric cryptography approach has a number of weaknesses, including:

1. The key used to encrypt message is the same one to decrypt the message.
2. There is no authentication check in the whole process, which means A has no idea if the message is received by B and B isn't sure the message is sent by A.
3. When A and B communicate for the first time, it may not be convenient to exchange the key, for example if one or other is in an insecure environment.

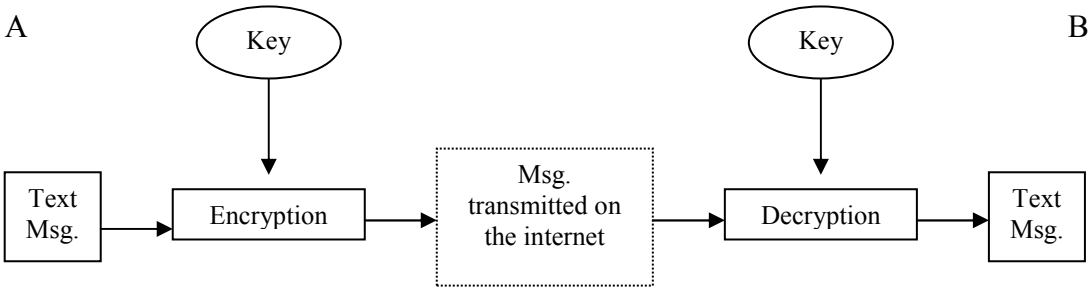


Figure 2.3 Secret key encryption

In addition, data transmission will not be secure if the key is lost or stolen. If someone gets the key illegally, he can send or receive any message which is not supposed to be sent or received by him.

2.2.4.2 Public key encryption;

Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

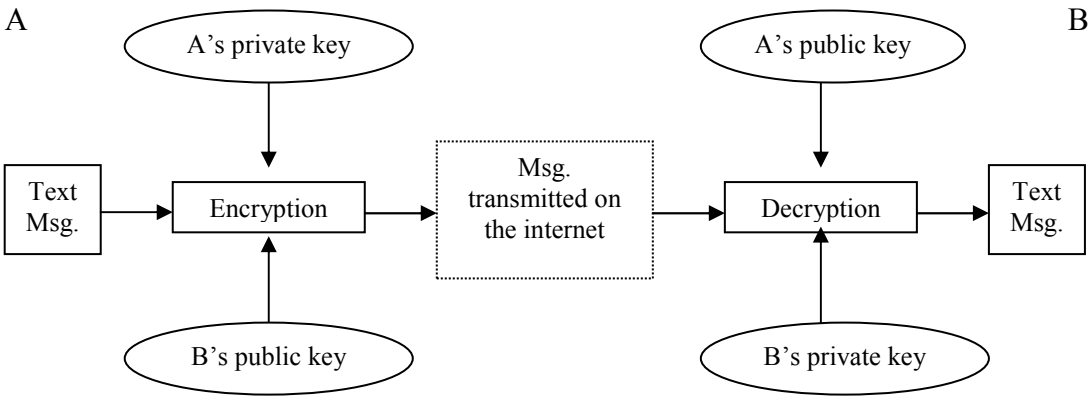


Figure 2.4 Public key encryption

The diagram above explains how the public key encryption works. A (sender) uses two different keys to encrypt the message because keys are working in pairs. One is A's private key which is to reassure B (receiver) the message is sent by A, not anyone else. The other key used to encrypt the message is B's public key, which is to reassure the message is decrypted by B, not anyone else. The data encryption and authentication check can therefore be done at the same time in asymmetric cryptography. The other advantage of public key cryptography is the convenience of exchanging public keys when contact is first made. We can use the communication established by A and B to explain this point. A (sender) sends its public key to B first for example. Then B (receiver) uses A's public key to encrypt its own public key and send back to A. A will use its private key to decrypt B's public key. Once two parties get each other's public key, the communication channel is set up successfully.

2.2.5 Internet fraud schemes

"Internet Fraud" refers generally to any type of fraud scheme that uses one or more components of the internet (e. g chat rooms, emails or website) to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (Criminal Division,U.S. Department of Justice). A list of fifteen types of attacks made through the internet is provided by Whitman and Mattord (2003,p64), which are briefly explained in the following passages.

(1) Malicious code

Virus, worms and Trojan horses are categorized in this type of attack. This attack programme is intent to steal or destroy information.

(2) Hoaxes

A real virus attached to a disguised massage which looks like from a legitimate source can fool users very easily. The damage will be done to everyone when users distribute the message to their friends and colleague.

(3) Back door

A back door attack is to have a programme (such as a key logging programming) installed on a computer. Then the programme sends out passwords to remote users so that the users can control and access the system.

(4) Password crack, (5) Brute force and (6) Dictionary

These three attacks focus on computing the password by guessing, using combinations and applying algorithms.

(7) Denial-of-Service (DOS) and Distributed Denial-of-Service (DDOS)

In a DOS attack, the attackers send out so many requests to the target that it results in a system crash or failure. A DDOS is an attack which against the target by controlling a group of computers at the same time but in different location.

(8) Spoofing

Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

(9) Man-in-the-middle

In the well-known man-in-the-middle or TCP hijacking attack, attacker sniffs packets from the network, modifies them, and inserts them back into the network. If this attack happens in the process of encryption key exchange, it causes worse damage. When sender and receiver exchange their encryption keys online, the attacker cut into the communication and get the packets from both sides. That is to say, the attacker becomes invisible and eavesdrop everything from both sender and receiver.

(10) Spam

Spam is called junk mail sometimes, but the spam attack is connected with Phishing emails which try to deceive users releasing sensitive information including personal and financial information.

(11) Mail bombing

Another DOS attack which uses a large number of emails to overwhelm the target's web-server system.

(12) Sniffers

A sniffer programme shows all the data going by, including passwords and the data inside of files, such as word-processing documents and screens full of sensitive data from application.

(13) Social Engineering

Within the context of information security, social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

(14) Buffer overflow

When the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure.

(15) Timing attack

Timing attack allows a web designer to create a malicious form of cookie to store on the client's system which allows the designer to collect information on access to password protected sites.

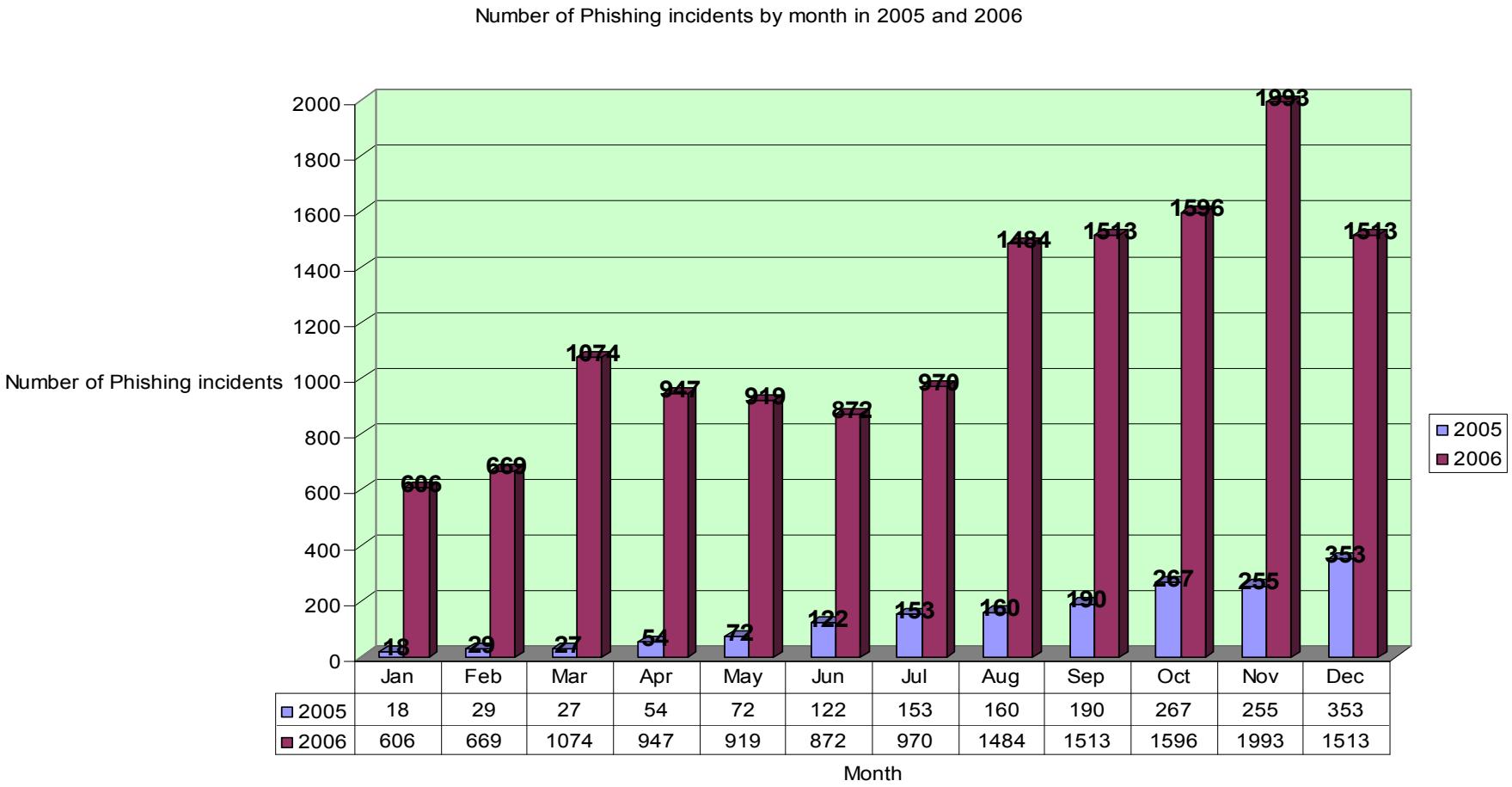
However, not all of these are useful for financial fraud, some being aimed at disruption of service or for other mischievous purposes. Internet fraud usually involves activities such as E-mail phishing, online auction and retail schemes, business opportunity schemes, identity theft and fraud, online investment schemes and credit/debit card fraud.

2.2.5.1 Phishing attack and spam emails

Phishing is the name given to the practice of sending e-mails at random, purporting to come from a genuine company operating on the Internet, in an attempt to trick customers of that company into disclosing information at a bogus website operated by fraudsters (APACS 2006). Phishing emails usually persuade customers to update their personal or account information by clicking links contained in emails. Once customers

click the links provide by phishing emails, they will be diverted to a malicious webpage which looks exactly the same as the original one. When customers update their information online, they never notice they are providing anything to criminals. Phishing attacks normally target customers rather than banks because banks systems are much more difficult to break. However, there were 14,156 phishing incidents targeted against UK banks and building societies in 2006 compared to 1,713 in 2005 (APACS, 2007). The big increase suggests that criminals see the activity as profitable and are becoming more sophisticated and specialized in their approach.

The figure on the next page shows the number of phishing attacks to internet users by month in 2005 and 2006 in the UK. We can see the number of phishing attacks increased from 18 in January to 353 in December in 2005 while from 606 to 1513 in 2006. It is worth mentioning that one single phishing attack could send out millions of emails. January 2005 had the least number of monthly phishing attacks for that year (18), but even this low number could still generate a large number of phishing emails. The total monetary loss would be considerable if, say, 1 in 1,000 people responded and released their personal or account information.



(source: APACS (2007))
Figure 2.5 Number of phishing incidents by month in 2005 and 2006

Let us have a look at profit made by spam emails according to the research results from (Pasquinucci 2007/2): imagine sending one million UCE (unsolicited commercial email) messages (this is a low number) of which only 10% arrive in the inboxes of recipients and 90% are blocked by anti-spam filters. Suppose that out of 100,000 messages delivered; only 0.1% led to an economic transaction. Each transaction is worth US$10 (again a low number). The gross profit for the UCE amounts to US$1000.

A typical operation of UCE involves three steps and characters. The vendor is the originator of the crime, who employs a UCE professional who performs two tasks: preparing the message (in such a manner that its true source is disguised) and selecting the list of recipients. These tasks can be delicate and technically difficult. Then there is the deliverer, likely to be a highly technical organization with the means to send out emails without being caught, often based in Eastern Europe or Asia.

With the increase in security awareness of internet users, phishing emails have become increasingly more sophisticated than before, with criminals refining their fraudulent schemes to keep capturing their victims. According to the 2006 Canadian Government report on Phishing, attacks can be divided into the following different types,

(1) Spear Phishing, which is described a highly targeted attack. This attack targets selected groups of recipients who share the same experience of some products, financial service and memberships. Just like standard Phishing emails, the message seems to be sent by a very trusted source. For example, an employer or a colleague who would be likely to send an e-mail message to everyone or a select group in the company (e.g., the head of human resources or a computer systems administrator) (Binational Working Group October 2006). Some criminals collect background information and try to personalize a phishing attack to a certain group of internet users, which increases the possibility of success.

(2) Redirection, whereby fraudsters use the technique to cause internet users to download malicious code into their computers unknowingly. Normally if users type a web address into a browser, the computer will direct users to the correct website. If the user's computer has been secretly infected by malicious code, the computer will be controlled by the malicious code and will direct the user to a phishing website, which is likely to resemble the original website that the user intended to browse.

(3) Keylogging or backdoor. Once the computer has installed the malicious codes, the keylogger will start to work automatically when internet users conduct online financial operations. When internet users try to log into their accounts by entering usernames and passwords, keyloggers begin to record the users' keystrokes, recognising the data used as the username and password and sending this information back to the fraudsters online. With this information, the fraudster can empty victims' accounts in few minutes. Even worse, fraudsters can remotely control victims' computers to do online transactions– referred to as a 'backdoor' operation. Sometimes the user who reports his doubts that his account has been illegally controlled is less likely to be believed at first because the financial institutions trace the transaction record back to that user's computer.

(4) Vishing or voice phishing, can work in two ways. One version is that customers receive phishing emails as usual indicating a problem with online accounts. Instead of providing a link in the email, it provides a telephone number and asks customers to call back to sort out the problem. When customers call back, they will be required to enter their account number and password by using the telephone keypad following the instruction given by a fake call centre. The other version is that fraudsters call customers directly and tell them to update or secure their account information immediately. Sometimes, fraudsters leave a voice message on customers' answer machines asking them to call the number provided. When customers call back, the person who answers pretends to be a customer service officer working in a call centre, who then asks for sensitive account information.

Voice phishing is easier to carry out than other attacks. Using simple software, criminals can set up an automated customer service line which sounds and feels as

professional as the ones used in most large firms. It is generally accepted that telephone banking makes customers feel more comfortable and reliable than internet banking. We call our bank very often to check the balance, transfer fund, pay bills, change billing address and etc. Sometimes, banks call customers to verify identification and offer advice on personal finance management. We are confident users of telephone banking because we know the whole process: how to enter account number, how to identify ourselves, how to choose service we need by press keypad. But we ignore an important issue: how do we know whom we are talking to on the phone - whether we are talking to the real bank staff or to someone else?

2.2.5.2 Trojan horses attacks

A Trojan, as is suggested by its name, is very good at disguising itself so that a user may never notice that their computer has been infected. For example, a person thinks he is downloading some software from the internet, but in fact, a Trojan hides in the software being downloaded. This explains where the Trojans gets the name, from the mythological Trojan horse that appeared to be a gift to the people of Troy but in fact contained a detachment of the Greek army, crouching in its belly and waiting until nightfall to come out and sack the city (Gralla 2006,p67).

Computers don't show any signs of Trojan infection. But Trojans allow attackers to take over computers remotely. One type of Trojan steals usernames, passwords and credit card information, and then sends them back to attackers automatically. Another type of Trojan, called a downloader, downloads malicious software and spyware to individuals' computers. Some Trojans, such as Back Orifice 2000, lie dormant until they are contacted by intruders (Gralla 2006,p67).

2.2.5.3 Worms and viruses

Worms are programmes designed to infect networks such as the internet by replicating themselves across different networks (Gralla 2006,p67). Viruses are malicious programmes that invade a user's computer causing many different types of damage,

such as deleting data files, erasing programmes or even destroying everything on a hard disk (Gralla 2006,p67).

The transmission mechanism is as follows. A worm arrives in people's email boxes disguising as a normal attachment. When the recipient opens the attachment, the worm is activated and begins searching the email software, particularly the address book. Worms will replicate themselves and send out disguised emails to the names on the mail list without the knowledge of the user. For the recipients of the emails, worms will do the same: infect machines, replicate and send out worm emails. Just like a snowball, the level of infection increases very quickly in a short time. Internet servers are not able to deal with the huge traffic of emails, some servers crash and systems fail. Alternatively, worms can provide a mechanism for distributing phishing emails.

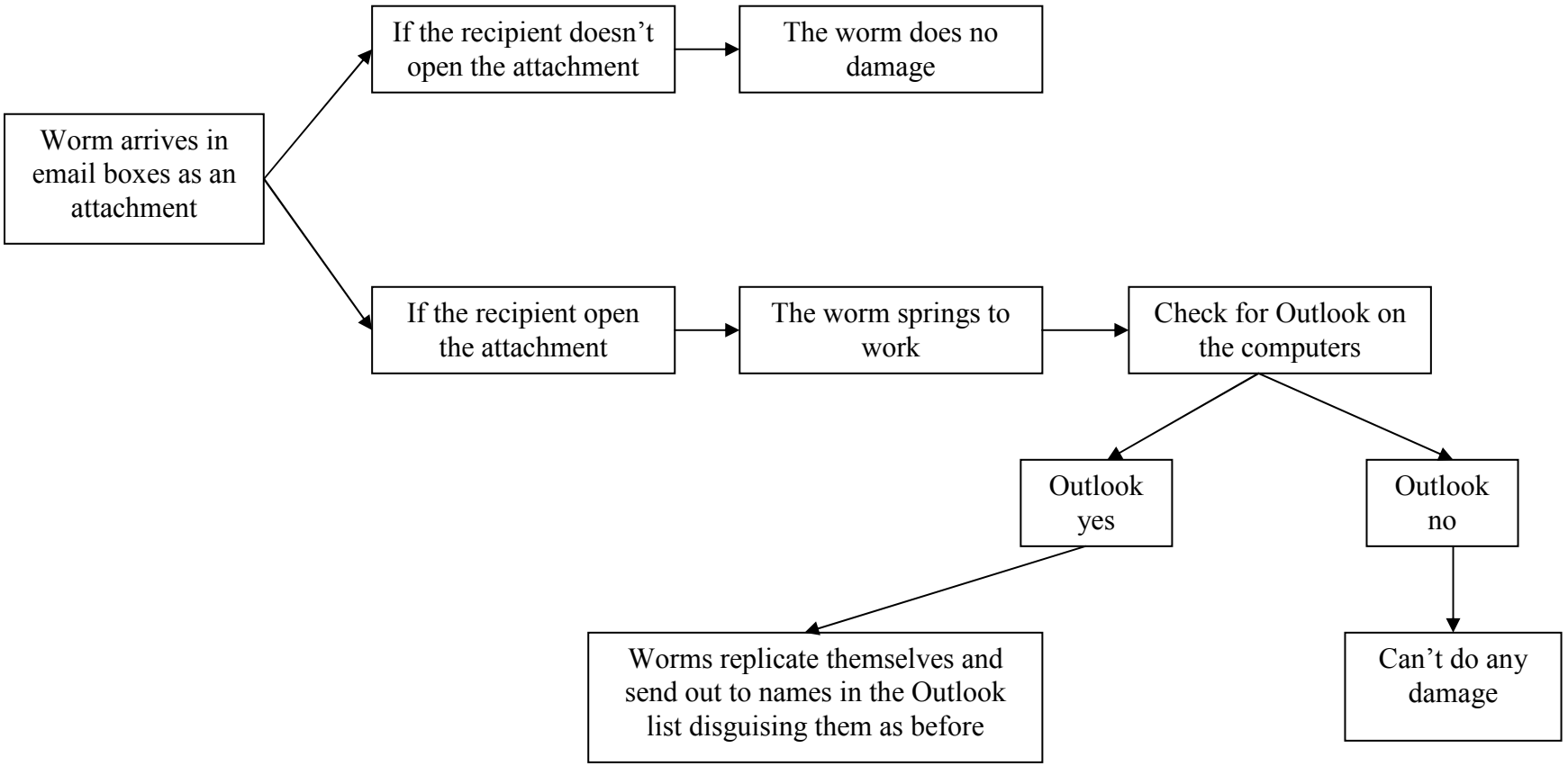


Figure 2.6 How worms attack from emails

In contrast to worms, which are designed to infect networks, viruses generally are malicious programmes designed to invade an individual's computer. Internet users can get a virus in many ways, including by opening an email, running an infected programme, downloading infected software or opening a document (such as a word document) that is infected with the virus (Gralla 2006,p67). After infecting a machine, the virus hides inside itself without any signs unless detected by virus checker, which normally checks files at the time of download (if applicable) or through system scanning. The virus will be activated when users run the infected programmes. Sometimes the first thing the virus does is infect other programmes on the user's hard disk by copying itself into them (Gralla 2006,p67). Viruses can cause much damage to computers and data by deleting and changing system files.

2.2.5.4 Instant messaging pests

Instant messaging is very popular means of communication on the internet because it is in real time, as opposed to emails. Using specific software, such as AOL instant messenger, MSN messenger, Yahoo messenger etc, we can communicate with anyone who uses the same software on the internet. According to the security firm IMlogic, AOL instant messenger, MSN messenger, Yahoo messenger each send more than one billion messages per day (Gralla 2006,p67).

Instant messaging has become a target for criminals. IMlog says that in 2005, instant messaging threats increased by 1,693% over 2004, with a total of more than 2,400 individual threats (Gralla 2006,p67). In the 12 months since September 2004, there was a greater than 2000% increase in the number of viruses reported that attack instant message and peer-to-peer networks (BBC 2005). Unfortunately, many users do not notice the massive growth in instant messaging pests. Fraudsters keep attacking vulnerable users using instant messaging techniques.

It is well known that files can be sent and received directly using instant messaging programmes on the internet. That is to say, spyware, virus or malicious code also can be sent out by instant messaging. Even some pests can send themselves via file

transfer automatically without knowledge of users. An example is W32.Funner worm, which can send a copy of itself by direct file transfer to everyone on the contact list of an infected computer. Like other types of worm we discussed in the former section, it looks into the name list of an instant messenger programme as soon as it infects the computer successfully.

2.2.5.5 Wi-Fi security

Development of network technology changes the way we access the internet, with an increasing number of people connecting wirelessly. The cost of setting up a wireless network is much cheaper than a wired one. More important, a wireless network is very convenient for users because anyone who is in range can access it, although they might need to know the appropriate WEP code in the case of closed networks. Such networks can also be used when we travel around, such as in airports, train stations and cafes etc.

The wireless technology is called Wi-Fi, which is an open technology. A wireless router broadcasts its presence to any device with a Wi-Fi adapter within its range, and if the router is unprotected, anyone who wants to can connect to it and use the network (Gralla 2006,p91). The very nature of Wi-Fi technology brings convenient access to anyone, including intruders.

A ‘war driver’ is the name given to a common type of Wi-Fi intruder. This person uses software to search unprotected wireless networks by driving in the cities and residential areas. Intruders can use antennas to catch many signals and networks. When war drivers target a home network, they are generally looking for personal information, while war drivers will steal business information when they break into a business network. Besides stealing information and privacy, intruders can use the network they break into for illegal operations, such as sending spam emails, attacking databases, spreading viruses etc.

Wi-Fi hotspots provide another way to get internet access using a wireless network. Each hotspot needs its own connection to the internet, so that people who connect to

the hotspot can in turn connect to the internet (Gralla 2006,p91). When a person uses a hotspot in the airport, his laptop is vulnerable to others who use the same hotspot because all of them are on the same network and need to share its bandwidth. For example, if a person turns on file sharing on his machine when he uses a hotspot, other users of the same hotspot may be able to break into and steal data from its hard disk.

Criminals can plant spyware and Trojans on other peoples' machine at the same hotspot which allows hackers to control computers remotely for illegal activities. At the same hotspot, fraudsters can capture the packets sent and received by anyone. These packets might contain personal information such as username, password, bank account numbers etc.

'Evil twin hack' is another type of Wi-Fi attack. In an evil twin hack, a hacker creates a twin of an existing hotspot to lure people into logging in to his hotspot rather than the real thing (Gralla 2006,p91). The hacker finds a popular hotspot and sets up a duplicate hotspot. In order to ensure users connect to the duplicate hotspot, hackers can add extra strength to his signal. Because of its stronger signal, users' laptops will connect to the duplicate hotspot automatically. Also, the hacker may jam the signals of real hotspot, ensuring that someone will connect to his hotspot instead of to the real thing (Gralla 2006,p91).

After users connect to the duplicate hotspot, hackers might take control of the machine, stealing personal and financial information. For example, the hacker can set up a fake login page to ask for a user's credit card number to make the payment required to buy time on the hotspot.

2.2.5.6 Browser weaknesses

Since the web browser is the working platform for financial internet transactions, it is no surprise that it is a target for fraudsters. Gralla (2006,p91) suggested three reasons to explain why browser-based attacks are on the increase: (1) the security level of the web browser is low and easily broken; (2) the web browser is the only means for individuals to surf on the internet and to make financial transactions online; (3)

hackers can attack the computer system through browser-based attack, for example Internet Explorer is tied into windows operating system directly and therefore provides a means of compromising the operating system.

One of the most common kinds of attack is called a buffer overflow attack, in which hackers write code that downloads from a website and floods a specific area of memory with so much data that it overflows into a nearby area of memory (Gralla 2006,p91). The malicious code hiding in the data flow can damage the computer and steal sensitive information. Another type of browser attack is called a drive-by download in which a malicious file including Trojans and spyware is downloaded and installed using the browser without the user's knowledge (Gralla 2006,p91).

2.2.5.7 Webjacking (internet hijacking)

By definition, the term "hijacking" refers to the seizure of a moving vehicle by use of force, especially to reach an alternate destination (McGillivray, Lieske Jul 2001). Webjacking, also known as internet hijacking, refers to the seizure of a domain name to force web traffic to an alternate web site location (McGillivray, Lieske Jul 2001).

With web design software, website and web pages are very easy to copy in a short time, especially as logos can be captured easily. Customers are not likely to find out whether the website is authentic or not because fraudsters copy the original website in entirety from the logo to the colour of the text. Nike.com was webjacked in June 2000 and customers who typed www.nike.com in their web browers were automatically directed to a web site in Scotland maintained by a group called S-11and hosted by Firstnet On-line Ltd (Harrison 2000). In this web jacking, both Nike and Firstnet On-line Ltd were victims. Nike lost its reputation and potential customers while Firstnet On-line Ltd was unable to serve its legitimate customers because its server was overloaded by redirected traffic (Harrison 2000). According to the Federal Trade Commission, page-jacking affects about 2% of the pages on the web (Pereira 1999; Pitofsky 1998).

2.2.5.8 Fraudulent online auction and retail schemes

Online auction and retail schemes induce their victims to send money for products selling online. After successful payment, promised products will either never be delivered or will be replaced by less valuable items such as counterfeit goods.

2.2.5.9 Business opportunity/"Work-at-Home" schemes online

This scheme is not a new one. It used to appear on the newspapers and magazines years ago. Fraudsters take advantage of the internet to advertise fake business opportunities that promise earnings of thousands of pounds/dollars a week or month working from their own home. Normally the fraudsters ask the respondent for their bank account details, ostensibly to transfer sales or commission proceeds into it, but the reality is that if the fraudsters get this information money will be speedily withdrawn from the recipient's bank account. Sometimes this type of scheme is referred to as a 'money mule'.

2.2.5.10 Investment schemes online

Sometimes online investment scheme frauds are referred to as "pump-and-dump" schemes or alternatively 'ramping'. Just like the business opportunity discussed above, online investment schemes use the internet to spread fake information to manipulate the market. For example, fraudsters can claim to be a company selling its stock, or they send out fake information to persuade online investors to buy a certain stock which they already hold. After the price increases, the fraudsters sell the shares making profits from the price difference.

2.2.5.11 Identity theft and fraud

Identity theft does not have to be connected to the internet but the internet can be a very efficient means of obtaining an individual's personal information and using it, for example to apply for credit cards, loans and also purchasing products using the stolen

identity. We will look at this scheme in detail when we discuss credit card transactions subsequently.

2.2.5.12 Credit/debit card fraud

Since the day that online shopping was introduced, plastic cards have provided an important means of payment because cash cannot be used on the internet. Bank card usage is therefore a prime target of internet fraudsters, particularly as it is difficult to provide a really secure system for internet card payment. There are different types of card fraud, such as lost and stolen card fraud, counterfeit card fraud (skimming), card-not-present fraud, mail-order non-receipt fraud and identity theft. These are discussed in more details in section 4.3 of chapter 4.

2.3 Online financial transactions

2.3.1 Two-way authentication in online banking

In making an online financial transaction, the first step is to be able to recognize and secure the identification of each party to the transaction. Where possible, financial institutions now use a two-factor authentication procedure to establish identity, privileges and secure the online financial environment. Here are the differences between the traditional password authentication and two-factor authentication.

Table 2.1 Two-way authentication

	How many factors do we need?	What are the factors?
Traditional password authentication	Only one factor	Password only
Two-factor authentication (T-FA)	Two factors	Something you know (a password) and Something you have (a physical device) or Something you are (biometric info.)

Although traditional password authentication did reduce the incidence of identity theft, two-factor authentication is believed to be much more effective. It is important component of the two factor procedure that the second factor relates to either a physical device or biometric information. If the second factor were to be of the same type as the first, this would not be considered two-factor authentication.

However, increasing levels of protection and security for customers, such as using complicated long digit passwords, changing password frequently, asking more than one question to confirm identification, would lower customer confidence. Complicated security systems drive customers away if there is no good balance between convenience and security. Online financial transactions are designed to reduce cost for banks and increase confidence for customers at the same time. If the customers are put off, they will just go back to branch banking, a system they have been used to for many years.

Some banks have started to try two-factor authentication for online banking, including some Hong Kong banks and the Bank of America. With 2.7 million internet banking customers, Hong Kong became one of the first places amongst the developed financial markets to establish clear regulations requiring all banks and customers to use two-factor authentication in online banking, together with digital certificates, SMS-based one-time passwords and security token-based one-time passwords (Banks move towards two-factor authentication. July 2005).

With 13 million online customers, the Bank of America adopted a different approach. Customers of the Bank of America pick an image, write a brief phrase and select three challenge questions (Banks move towards two-factor authentication. July 2005). This method not only lets the bank check customers' identification, but also lets customers check if they are dealing with the bank's authentic website. Customers can ask the bank to show the images and phrases they registered while banks can ask customers to answer challenge questions. The following webpage shows an image and a brief phrase selected by customers at the first registration (Banks move towards two-factor authentication. July 2005):

Figure 2.7 Two-factor authentication adopted by the Bank of America

Vance, J. (Jun 5, 2006) noted this is more secure than traditional password authentication because it relies on what you know (your password) plus other things you know (answers to questions). At a cost of about $1 per user per year, the solution should easily pay for itself with reduced fraud (Vance Jun 5, 2006).

2.3.2 The black market

On 17th, January 2007 (Greenemier, Hoover 12 Feb 2007), retailer TJX disclosed that the computer systems storing customers' data had been broken into. The intrusion involved systems that handled credit card, debit card, cheque (check) and return transactions for T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico, and also the Winners and HomeSense stores in Canada. TJX said that the exposed data covered 2003 and the period from mid-May through December 2006 (Joris 18 Jan 2007). The hackers were successful in selling some of this information on the black market.

Hacking into large company databases can be extremely lucrative. The online black market offers all kinds of illegal products and services, the following being a typical price list from online black market in the US in 2007 (Greenemier, Hoover 12 Feb 2007):

Table 2.2 The price list from online black market

Trojan programme to steal online account information	$980--- 4,900
Credit card number with PIN	$490
Billing data including account number, address, social security number, home address and birth date	$78---294
Driver's license	$147
Birth certificate	$147
Social security card	$98
Credit card number with security code and expiration date	$6---24
PayPal account log on and password	$6

With the attractive profits from online black market, more and more hackers conduct well organised fraudulent schemes and use online payment systems to do trades. One of the direct approaches taken by hackers is called 'Ransom Scams', in which criminals break into company's system and encrypt data using malicious programmes and then demand money to provide the decryption. Similar scams using direct approach are not very common because they require a direct connection between the victims and the fraudsters – clearly this poses a high risk. A more common way for hackers to make money is by selling stolen data on the black market.

Listed in the table above, we can find all kinds of data for sale on the online black market, such as Credit card number with PIN, Billing data including account number, address, social security number, home address and birth date. General speaking, credit card information is sold in bulk because any card could be cancelled or 'hotlisted' (Greenemier, Hoover 12 Feb 2007). Although prices listed on the website are different and often depend on the quality of the data, basic card information can go for as low as $1 a card (Greenemier, Hoover 12 Feb 2007).

Specific, members only websites exist for fraudsters to trade. Registered members of the website use peer-to-peer payment system just like selling and buying on E-bay. The average life expectancy for such sites is about six months and they need to reroute

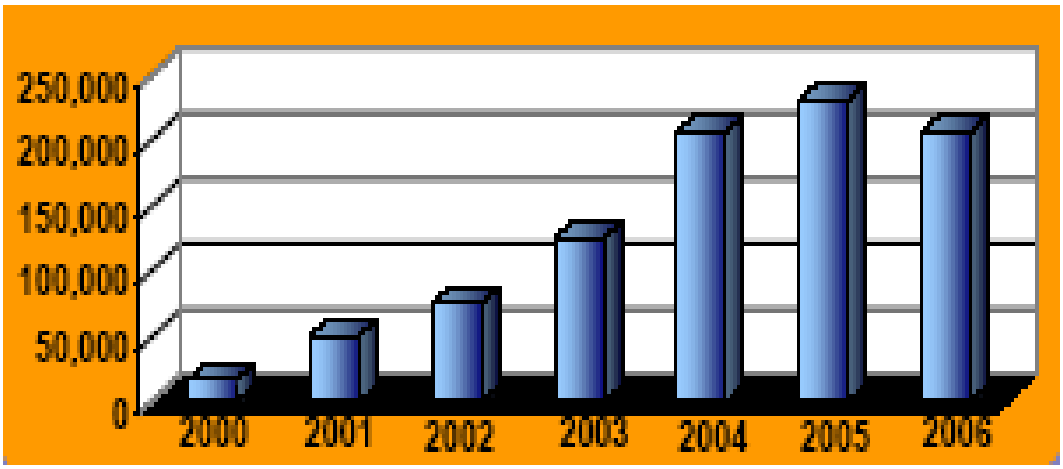
to a new server to escape law enforcement (Greenemier, Hoover 12 Feb 2007). Criminals split large transactions into small ones to avoid the attention of banks.

Another commodity offered on the online black market is malicious software including viruses, worms and Trojans. According to Raimund Genes, a flaw in Microsoft's new Windows Vista operating system was found for sale on a Romanian website forum for $50,000 in December 2006 (Greenemier, Hoover 12 Feb 2007). Criminals target and discover vulnerabilities and weaknesses of operating systems, software and any IT products. High price motivates more and more criminals, for example security vulnerabilities were selling last year for as much as $20,000 to $30,000 each on the internet (Greenemier, Hoover 12 Feb 2007). Unfortunately, there is little law enforcement to stop people finding security vulnerabilities.

2.4 Internet crime worldwide

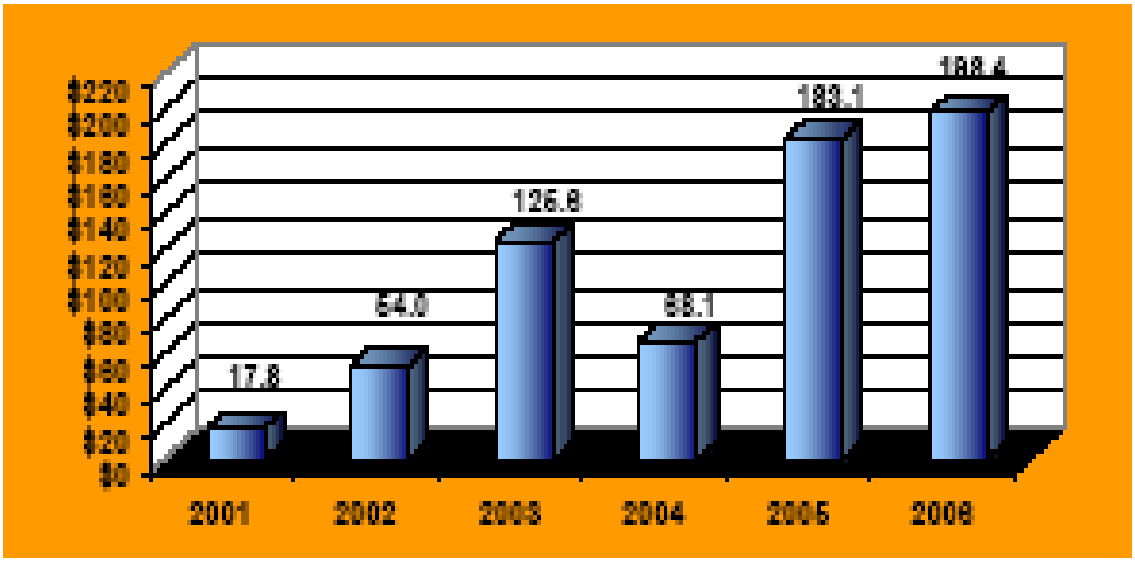
2.4.1 United States

In the US, various agencies have been created in response to internet fraud. For example, "The Internet Crime Complaint Center (IC3), which began operation on May 8, 2000, as the Internet Fraud Complaint Center was established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime" (IC3 2006). Complaints can be submitted mainly on the website of IC3. After the submission of complaint, the information is recorded and categorized, then forward to the related or regulatory agency. The following charts will help us understand the current status of internet crime in US.



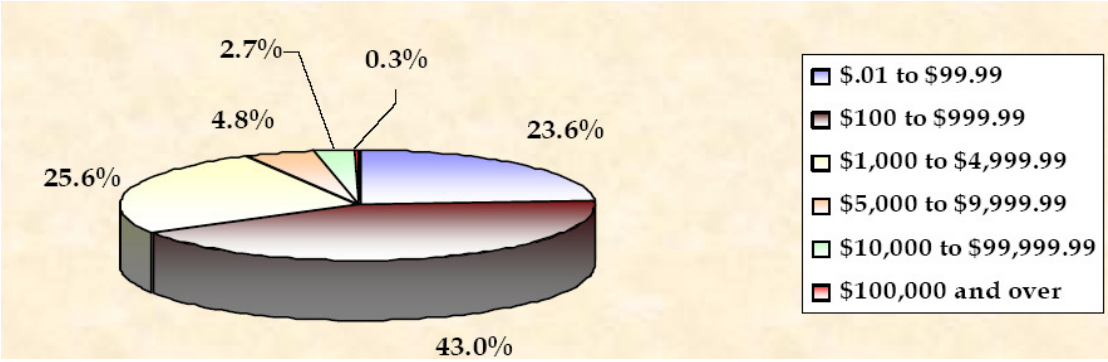
(source: (IC3 2006))
Figure 2.8 Yearly Comparison of Complaints Received Via the IC3 Website

From January 1, 2005- December 31, 2005, IC3 received 231,493 complaints online which is an 11.6% increase over 2004, when 207,449 complaints were received (IC3 2005). Additionally, we can find out that complaint submissions have increased annually from 2002 to 2005 in the chart above. The number of complaints in an average month was 19,291 in 2005 (IC3 2005).



(source: (IC3 2006))
Figure 2.9 Yearly Dollar Loss of Referred Complaints (in millions)

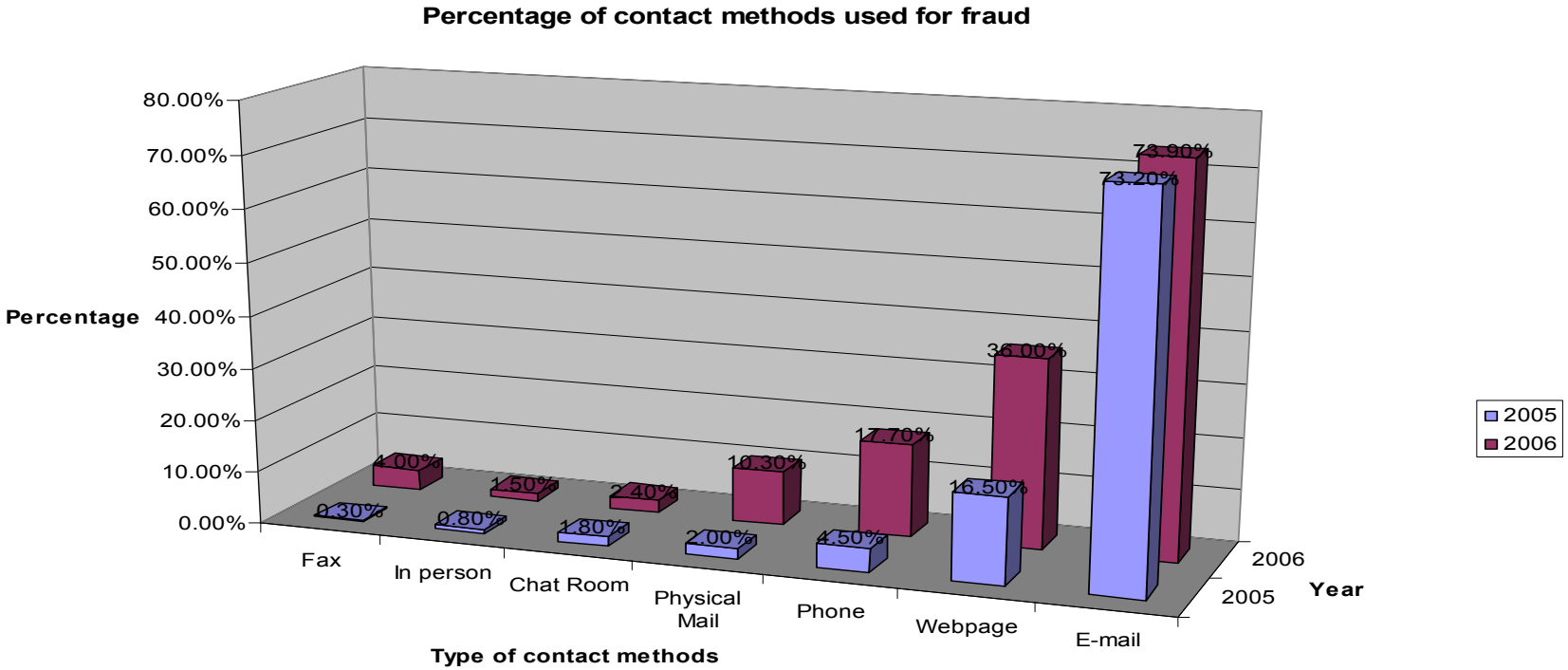
The total loss of fraud in 2005 was $183.12 million and it was significantly greater than 2004 which reported a total loss of $68.14 million. This result was due to a number of cases in 2005 which reported losses in the millions of dollars (IC3 2005).



(source: (IC3 2005))
Figure 2.10 Percentage of referrals by monetary loss

Twenty four percent (23.6%) of these complaints involved losses of less than $100, and (43.0%) reported a loss between $100 and $1,000 (IC3, Internet Crime Report, 2005). That is to say, 66.6% of these cases involved a loss of less than $1,000. About a third of the complainants reported high dollar losses, with 25.6% indicating a loss between $1,000 and $5,000 and only 7.8% indicating a loss greater than $5,000 (IC3, Internet Crime Report, 2005). With extremely low cost and high efficiency, criminals can net many victims in couple of minutes by sending phishing emails.

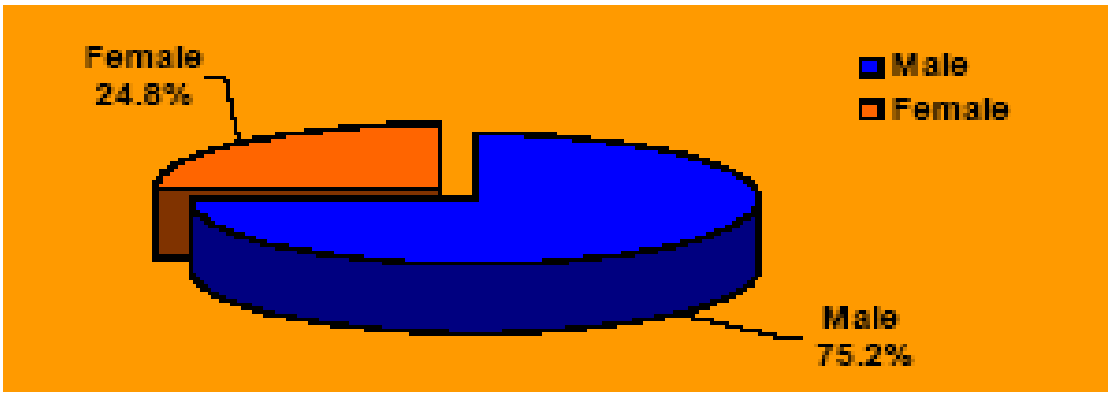
For the criminals in cyber space, criminals usually chose e-mails and websites to contact their victims. Electronic mail (E-mail) and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, 73.2% of complaints reported that they had e-mail contact with the perpetrator and 16.5% had contact through a web page (IC3 2005).



	Fax	In person	Chat Room	Physical Mail	Phone	Webpage	E-mail
2005	0.30%	0.80%	1.80%	2.00%	4.50%	16.50%	73.20%
2006	4.00%	1.50%	2.40%	10.30%	17.70%	36.00%	73.90%

(source: IC3 (2005, 2006))
Figure 2.11 Contact methods used for fraud

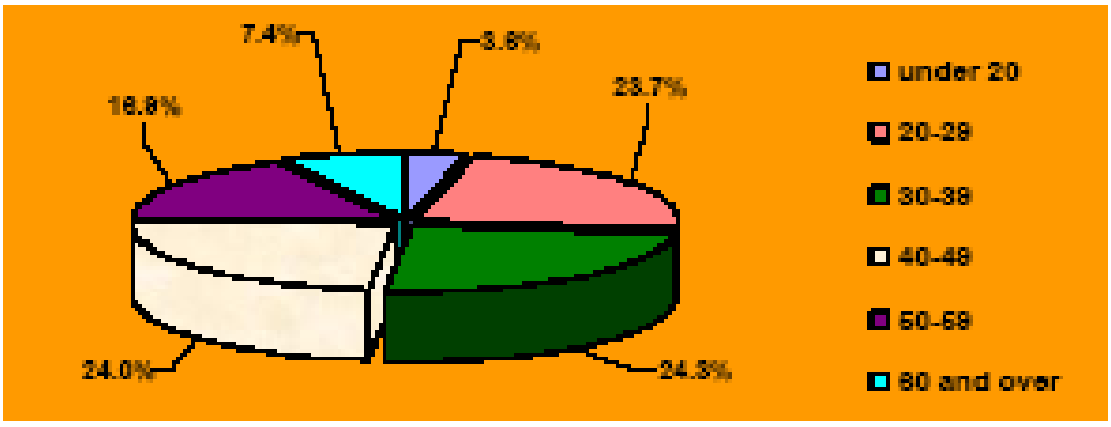
The following pie charts also show the gender difference of perpetrators and age demographic of complainants. In the following figure, 75.2% perpetrators were male and 24.8% were female.



(source: (IC3 2006))

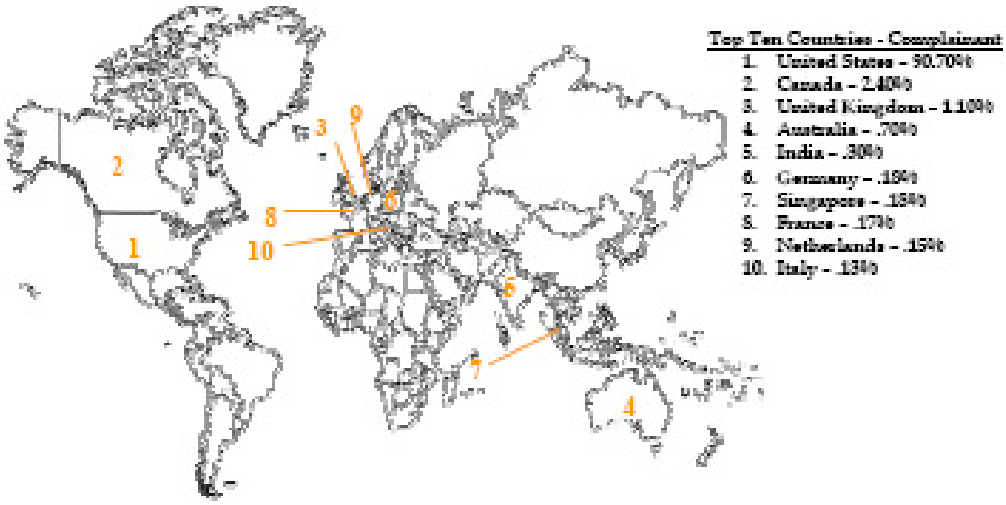
Figure 2.12 Gender of perpetrators

Six age groups were shown in the following figure: under 20 (3.8%); 20-29 (23.7%); 30-39 (24.3%); 40-49 (24.0%); 50-59 (16.8%) and 60 and over (7.4%).



(source: (IC3 2006))

Figure 2.13 Age demographic of complainants



(source: (IC3 2006))

Figure 2.14 Top ten countries—complainant

Table 2.3 Top ten countries – complainants (as used in Figure 2.14)

1. United States	90.70%
2. Canada	2.40%
3. United Kingdom	1.10%
4. Australia	0.70%
5. India	0.30%
6. Germany	0.18%
7. Singapore	0.18%
8. France	0.17%
9. Netherlands	0.15%
10. Italy	0.13%

2.4.2 Asia (China mainland and Hong Kong)

In China, internet banking services first emerged on the mainland in 1999 (Lee, Kim 2010). In the following five years, more than 20 banks in China began to offer online financial transaction services. Internet banking was accepted gradually by customers in the beginning but is now in widespread use. As expected, criminals exploit the vulnerabilities and weakness of online financial transaction systems. The figures in the

following table came from a survey result concerning the perception of the impact of online vulnerability conducted in 2006. This survey focused on the past fraud experience of private sector organisations of different sizes and showed the extent to which the respondents perceived the threats of computer related fraud both in the China mainland and in Hong Kong.

Table 2.4 Perceptions Relating to Electronic commerce and computer-related fraud in Hong Kong and China
(source: KPMG HK (2006))

Area	**China mainland**	**Hong Kong**
Unauthorised manipulation of computer data	35%	37%
Unauthorised computer programme change	29%	41%
Internet banking fraud	19%	47%

- 35% and 37% of the respondents believed that unauthorised manipulation of computer data would create great risks to their organisations in mainland China and Hong Kong respectively;
- 29% and 41% of the respondents believed that unauthorised computer programme change would create great risks to their organisations in mainland China and Hong Kong respectively;
- 19% and 47% of the respondents believed that internet banking fraud would create great risks to their organisations in mainland China and Hong Kong respectively;

In Hong Kong, IT technology crime is commonly known as technology crime or computer crime. There are different types of criminal activities: Hacking (Unauthorized access, access with criminal intent); Internet Fraud; Bogus Websites and Internet Banking fraud. Some are traditional crimes committed through the internet, some use computers to commit crime whilst some crimes are targeting against computer system. The following table was found on the website of Hong Kong Police Force and illustrated the figures of Technology Crime from 2000 to 2004:

Table 2.5 Technology Crime Statistics in Hong Kong
(source: Hong Kong Police Force (2006))

Title of Offence	2000	2001	2002	2003	2004
Unauthorized Access to Computer by telecommunication	275	33	26	47	11
Access to Computer with Criminal Dishonest Intent	-	81	138	356	329
Criminal Damage	15	27	16	16	11
Obtaining Property by Deception	29	32	45	86	105
Obtaining Services by Deception	-	33	19	17	15
Thefts (E-banking related)	0	8	6	8	19
Others*	49	21	22	58	70
Total	368	235	272	588	560

*Others include traditional offences such as criminal intimidation, using a false instrument etc.

For offence called “e-banking related”, the figure in 2004 increased more than double size of the figure in 2003. These figures explained that internet crime is still at its early stage in Hong Kong. Compared to UK and USA, the loss and damage caused by technology crimes is relatively small but will undoubtedly increase if preventative action is not taken.

2.5 Online retailers

A survey by ‘Computer Fraud and Security’ in 2007 showed that 64% of British-based E-commerce retailers had been defrauded, claiming that online retailers were losing £580 million per year in the UK from cyberfraud (Online retailers in UK lose £580 million to fraud. 2007). Caunter (2001) estimated that in 2001, of the 27 billion credit card transactions worldwide, 2%, or 540 million of these transactions took place on the internet. Statistics indicate that e-commerce fraud is 10 to 20 times more likely than in face-to-face transactions, with some research claiming fraud rates as high as 5-10% such as experienced by Expedia. Internet fraud is easier to conduct and harder to detect than in face-to-face transactions. Without the physical environment that has provided the background for transactions for generations, people become more vulnerable and abandon common sense on the internet, a virtual society.

Online merchants have already taken measures to detect online fraud using security software. Repeated attempts to purchase on the same card number, delivery addresses that differ from the card billing address and the use of anonymous e-mail accounts are parameters that can be set to alert retailers to the possibility of fraud; limits on the value of transactions made during certain hours of the day and at the weekend when fraud is more likely to occur can be specified, as can blocks on transactions from countries with which the merchant does not wish to trade (Wilcox, P. 2000).

Visa international launched a website to assist merchants to protect and store data. Merchants can get an evaluation of their level of security through Visa's website by completing a questionnaire. But John Pescatore, an analyst with the Gartner Group, explained that the Visa programme would not be very helpful to Visa merchants because Visa International requires merchants to upgrade their security without reducing Visa transaction fees or chargeback rates on fraudulent transactions (Gengler 2000). This practice would benefit customers and card issuers but not merchants, who might have to invest lot of money to upgrade their security. If Visa were to reduce their transaction fees or chargeback rates, merchants would be more motivated to upgrade their security.

2.6 Customers perception

2.6.1 Customers' adoption of online financial transaction

In the previous studies on the adoption of online transaction systems, many factors have been analyzed and tested to try to understand the slow rate of adoption. Howcroft *et al*. (2002) studied the demographic characteristics of respondents including gender, age, annual income, level of education, ownership of financial products and compared the results with national average for the UK. The result shows that middle age groups (between 35-54 years old) who have higher income and a higher possession rate of information technology products are very likely to adopt internet banking. For these relatively high profile customers, the time saving and convenience of internet banking is attractive. In addition they can afford to use up-to-date security software and latest IT products to provide secure online banking at home.

Besides the demographic characteristics of customers, many studies have focused on customers' attitudes to and behaviour towards the adoption of online financial services. Black N.J. *et al*(2001) conducted a qualitative study that employed Roger's model (Rogers 1962) to analyze customers' adoption decisions, but perceived risk was added to the model as an extra construct to capture the degree of security relative to other banking channels. This was found to be significant, confirming the results of other studies which indicate that customers are concerned with online security, particularly of online banking (Jayawardhena, Foley 2000; Rotchanakitumnuai, Speece 2003). Similarly, a survey was conducted to acquire data from customers who were not internet banking users, the results indicating that "lack of adequate security" was more highly weighted than any other factor Gerrard, P. *et al* (2006).

From the figures of different customer groups released by APACS on 24th August 2007, the biggest increase in adoption of online banking in the five years to 2006 is from the over-55 age group. The five-year growth statistics for online banking show that the number of adults in the UK using online banking has increased by 174 per cent from 6.2 million in 2001 to 17.0 million in 2006, including a 350 per cent increase in usage amongst the over 55s (Politics.co.uk 24/08/2007).

Table 2.6 Internet banking users in various age groups
(Source from Politics.co.uk (24/08/2007))

		2006	2001	Change
People using online banking		17.0 m	6.2 m	+174%
People banking online by age group	16-24	1.8 m	0.8 m	+125%
	25-34	4.1 m	2.1 m	+95%
	35-44	4.2 m	1.4 m	+200%
	45-54	3.1 m	1.1 m	+182%
	55-64	2.1 m	0.4 m	+425%
	65+	1.5 m	0.4 m	+275%
People using telephone banking		15.7 m	11.5 m	+37%
People shopping online		28.3 m	11.0 m	+157%
Purchase per online shopper		£ 24.0	£ 8.4	+186%

Also, we can see a great increase in the population of online shopping in 2006, which is 157% higher than in 2001. While the debit card payment is more popular than credit

card payment on the high street, credit cards are more widely used on the internet, with 252 million transactions last year - an increase of 29 per cent on the 2005 figure (APACS 2007). Customers may well choose to use credit cards on the internet because of the increased protection credit cards offer, such as AVC (address verification check), Visa and Master card verification etc and insurance against faulty goods or fraudulent transactions. Since most credit card providers use neural network software, which track spending patterns and monitor unusual activity on accounts, the largest recent losses are with debit cards (Jerving 2007).

Neural network software records spending patterns and builds a specific profile of each account. For example, how much money customers spend every month on average; whether customer go shopping usually in workdays or weekends, whether transactions are normally made in the morning, afternoon or at night; where common purchases take place, eg on the high street or on the internet, etc. With a spending profile generated for each customer, neural network software examines each transaction request and assesses its authentication. If the transaction is suspicious, credit card providers will contact customers immediately to ask for further confirmation or wait for them to call to provide authentication.

2.6.2 Public awareness and perception of biometrics

In information technology, biometric authentication refers to technologies that measure and analyzes human physical and behavioral characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. Worried about growth of internet fraud, people are seeking a unique way to identify themselves. Biometric data are attached to each individual physically since someone is born and it is like secret code for each person.

The earliest public awareness of biometric data is probably the use of fingerprints to solve crimes. More recently, biometric technology can be found on certain electronic devices such as laptops, PCs, alarm and security systems. In addition, many people

will already have been exposed to them in contexts such as air travel and immigration (Furnell, Evangelatos 2007/1). For the majority people who have no actual experiences of using biometric detecting equipment, it's not clear that they are ready or not for this new technology at the time of writing (2009/2010).

Furnell, S. and Evangelatos, K. (2007/1) conducted a survey on the use of biometric information both by post and online in 2006. The majority of responses came from females (57%) and 81% of the overall respondents were aged under 30 which means the respondents were part of the generation that grew up with information technology. When respondents were asked whether or not they were satisfied with the current technology to fight theft (online banking and ATM withdrawals), 45% of the respondents said 'no' while 26% said 'yes' and the rest were not sure (Furnell, Evangelatos 2007/1). It is clear that respondents had less faith in the then current technology used for authentication. In another study (Consumers losing trust in online banking: Survey. 2007/2), 52% of respondents said they were "less likely" to sign-up for online banking and more than half of respondents (58%) also believe that banks should have stricter authentication controls for telephone banking. Biometric data have the potential to provide a solution to some of these concerns.

2.6.3 Internet psychology (strangers' talk on the train)

The internet provides a special psychological environment for users that is quite different from the physical world. McKenna, G. *et al* (2002) suggest four factors to explain the differences between internet interaction and face-to-face interaction: 1. greater anonymity; 2. the diminution of the importance of physical appearance; 3. greater control over the time and pace of interactions; 4. the case of finding similar others. Online customers, who are trying to manage their finances on the internet, are attracted mostly by convenience and independence provided by internet.

People can easily keep their anonymity, which on one level can be seen as a protection for everyone but on another level is a licence for deception. We can use fake address and name, even personal information to get an email account, to register in a chat room, etc. Greater anonymity seems to protect everyone's privacy on the internet. But

hiding everyone's identity means there is no authentic or real information on the internet which is dangerous for everyone. From this aspect, internet becomes a place full of assumptions, imaginations, uncertainties even lies.

Greater anonymity misleads internet users to believe that they are safe and protected on the internet. At the same time, people are very likely to ignore 'strangers-on-a-train phenomenon'. When two strangers meet on the train, they talk to each other and disclose some personal information because they think they will never meet again or there is a slight chance they meet again. A similar perception also happens on the internet. Online users don't show their physical appearances to each other when they are chatting on the internet. Joinson (2001) suggests that computer-mediated communications and general internet-based behaviour contain high levels of self-disclosure. People are more likely to disclose personal information on the internet than in face-to-face interaction.

Ignoring the potential threats coming from the internet and underestimating the harm causing by someone hidden, people are caught out by criminals much easier than in the real world. For example, if someone approaches you in the street offering a big amount of money if you let him to use your account to make a money transfer, most of us would become suspicious and walk away. But the result might be different when the same story turns up on the internet. Internet users still reply to Phishing emails, such as 419 or Nigeria fraud in which fraudsters asked for help in transferring billions of dollars out of the country into an individual's personal account, for a sizeable fee. Those that responded with their bank account details found that money was removed from their accounts rather than paid into them.

2.6.4 Detecting deception on the internet (vulnerabilities of people)

Deception describes the conflict between two parties: a deceiver and a target. Theory of deception states that individuals detect deception by noticing and interpreting anomalies in their environment in light of the goals and capability for action that they ascribe to others with whom they interact (Grazioli 2004). During the process of the

detecting deception, individuals seek clues of deception by comparing new information with knowledge and experiences they already have.

In 2004 an experiment was carried out by Grazioli, S. (2004)in an American university involving 80 MBA students. These participants were recruited from MBAs specialising in information technology and had been using the internet for about four and a half years. The researcher built a fake website which was virtually identical to one selling used laptops. The participants were asked to buy a used laptop for their friend on the internet. They were given either the real website or the fake website at random. If they got suspicious about the website, they were instructed not to place an order. Otherwise, they would place an order online for their friends.

The result of the experiment is shown in the following table:

Table 2.7 The experiment of fake website
(Data source from Grazioli, S. (2004))

	Fake website (40 participants)		Real website (40 participants)	
Think its fake	12	30%	13	32.5%
Think its real	22	55%	15	37.5%
undecided	6	15%	12	30%

With other statistics figures coming from the experiment, Grazioli, S. (2004) suggested that as a group (i.e., as an average) these subjects cannot discriminate between the genuine and the fake site. The participants in the experiment are well educated and professional. Most of them have had online shopping experiences before. Unfortunately, the results discovered they are still poor at detecting deceptions on the internet.

For other online users, who might be less educated and less experienced on the internet, it seems impossible for them to detect deception and recognize fake information on the internet. Although researchers set some clues on the fake website to remind participants to be alert, these clues are very different from the clues we are used to in the physical world to check authentication. The types of checks that might

be regarded as ‘common sense’ in the real world are not so easy to apply in the cyber world.

2.7 Conclusions

The internet has changed the way we do business forever. In the physical world, criminals can only target certain areas of commerce, such as warehouses, outlets and offices. They can’t control or change the whole business organization in every detail. But in the online environment, criminals can pose as authentic owners and pose a much greater threat to merchants and customers. Cyber criminals not only steal money and information from customers but can also ruin the reputation of online merchants. Compared to fraud schemes using the telephone and post, online fraud is more effective and cost effective. Anyone who accesses the internet could become a potential victim.

The central question at the heart of this dissertation, as outlined in chapter 1 (section 1.3) is to explore both the susceptibilities and the attitudes of individuals to electronic fraud in relation the statistical data, the surveys undertaken in this study, the robustness of the electronic systems and the responsiveness and ‘user friendliness’ of the financial institutions in matters such as compensation and willingness to help.

As is evident from section 2.6, previous academic studies in these areas are thin on the ground, with most of the attention being directed at the attitudes of consumers to internet banking rather than to fraud and no studies dealing directly with actual cases of fraud. It is this gap in the literature which this study aims to address.

This chapter focused on generic issues related to IT technology, network security, online transaction environment and customers’ perception. The next chapter focuses on the legal environment surrounding online and automated financial transactions.

Chapter 3 Legal Environment Surrounding On-line and Automated Financial Transactions

3.1 Introduction

The full legal framework covering credit card and on-line financial transactions is extensive as it covers the actions of the counterparties and intermediaries (eg Visa, Mastercard), banking and other financial regulation (such as usury restrictions where applicable, eg in Arkansas and Louisiana), fiscal arrangements (which explain why many US credit card companies are based in the state of Delaware), freedom of information, company law, contract law, bankruptcy law and elements of international law. The type of legal system also has a bearing on the way that the law evolves, particularly in response to innovative financial structures and processes. This is particularly apparent in the differences between the dual legal systems of the US and the UK, where statute law is supplemented by case law, compared to the codified system of countries such as China where new situations have to be treated in the context of statute law alone.

In this chapter, we start by looking at the financial flows involved in online transactions and card payments, and proceed to look at the legal issues that surround these. In the case of UK and US law, we explore some legal cases which illustrate the exposures and obligations of the parties to the transactions. We then explore some of the differences that exist in China, where in general the system is less favourable to private individuals who have suffered fraud.

3.2 Financial flows to online transaction counterparties

Generally speaking, there are four main parties involved in online financial transactions: banks or credit card companies, online merchants, financial intermediaries or clearing organisations (such as Visa) and online customers. Figure 3.1 shows the effective financial flows between these three parties (note that the financial intermediaries, which act as clearing organisations, are not shown):

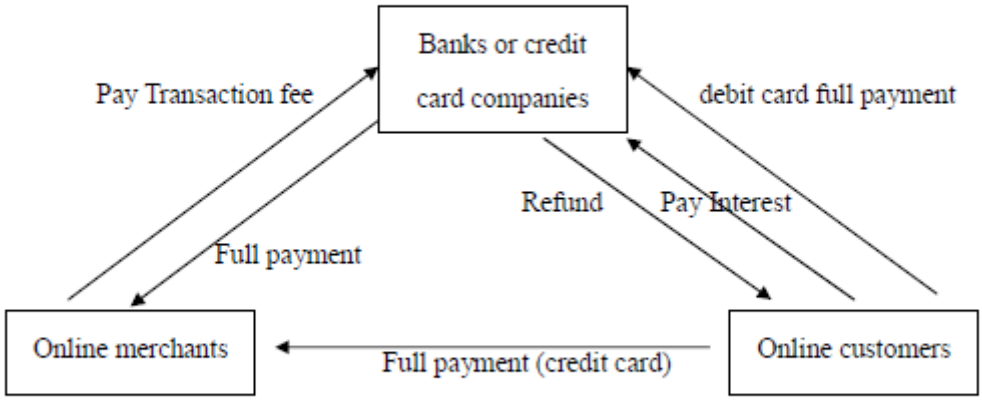


Figure 3.1 Financial flows to online transaction counterparties

Credit card companies derive their income in roughly equal measure from the merchant charge made to the seller and from the interest from customers who do not pay off their full balance on a monthly basis. Both banks and credit card companies rely on the high interest rates charged to customers. This high level of interest compensates for total fraudulent transactions, as can be inferred from the spectrum of credit card interest rates on offer in the UK, where 'credit builder' cards issued to high risk customers currently attract an interest rate of around 40% p.a. whereas platinum cards for low risk customers have rates less than half this.

In the authorisation process for a particular transaction, the approving party (the credit card company or bank) can make two types of error, ie:
1) They reject an online transaction when it is good (type I error);
2) They accept an online transaction when it is fraudulent (type II error)

The loss and profit from 1) and 2) are significantly different. When 1) happens, they might lose interest (averaging 2-6%) from customers (ie from those who would not have paid off their credit card balance) and they lose the merchants' fee (typically 2-6%). When 2) happens, they lose almost all the value of the transaction because they have to refund full payment (94-98%) to the customer but only make profit from the merchants' fee (2-6%). However, if the merchant has not followed proper verification

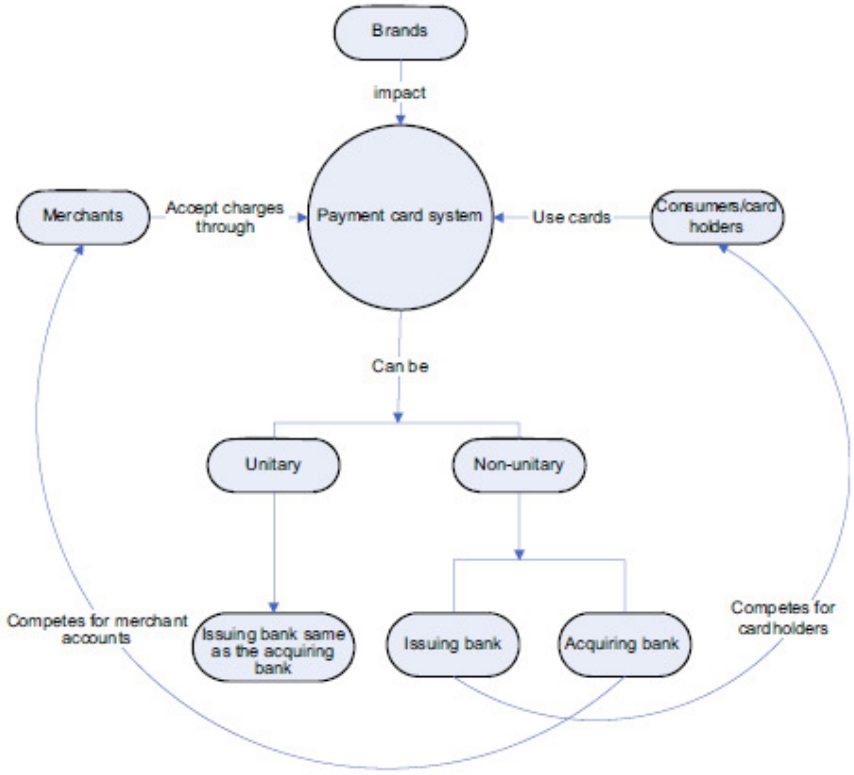
procedures or is responsible for the failed transaction the full cost may be borne by the merchant. As with any risk sharing arrangement there may be a rôle for a financial intermediary such as an insurance company, a view that was echoed by professionals working in the financial sector in China. For debit card transactions, there is a direct link to the cardholder's bank account when payment is made. This guarantees that there are sufficient funds available to settle the transaction, even though the transaction might be contested by the account holder if the transaction proves to be fraudulent.

3.3 Legal framework

From the point of view of fraud, in the US and Europe as a general rule the legal framework is angled towards benefitting the consumer in that it provides the individual considerable protection against unauthorised transactions. However, in China the extent of exposure is more dependent on the terms of the credit card agreement between the individual and the credit card company.

3.3.1 USA

The following figure shows the payment card industry features, in particular displaying the interrelationship between consumers and merchants in the United States:



(source: (Morse, Raval, 2008))
Figure 3.2 Payment Card Industry Features

Besides the benefits to each party provided by card payments / transactions, the risks concerning information security and fraudulent transactions affect the development of card payment systems. Unauthorized charges usually are caused by illegal access to customers' data including personal and financial information. Fraudulent cases involving lost and stolen cards, counterfeit card and card-not-present transactions would damage customers' confidence if the losses involved were experienced only by the consumer.

As applied by the payment card industry in United States (Morse, Raval, 2008), the consumer side of the trust equation has been addressed quite early (in 1970's) in the history of credit cards through legislation favouring card holders by limiting their liability for unauthorised charges. For example, 'zero liability' policies, have been used to protect consumers' trust and encourage them to use card payment systems. Essentially, under the USA system, the merchants have to bear the costs caused by unauthorised transactions respectively in (1) losses of goods / services; (2) charge back plus additional fees and penalties.

Furthermore, as discussed by R. Steennot (2008), the United States Truth in Lending Act (1968) applies to credit cards and contains a liability regime which is very favourable for the card holder. In other words, original card holders will not be held liable for the fraudulent transactions as long as they notified the financial organizations. For fraudulent transactions that occurred before notification, the card holder's liability is limited to $50. In practice many issuers will waive this small amount and simply write off the fraudulent transactions from the customer's account. Defrauded customers would get a full refund provided they signed a confidentiality document as required by the banks.

Unfortunately, not each case is settled to the customer's satisfaction. On 7th Feb 2005, a Miami business sued Bank of America for over $90,000 (Finextra, 2005), due to an illegal transaction on the company's online banking account by Latvian cybercriminals. According to the report, $20,000 had been withdrawn by the criminals before the account was suspended. Experts called in to investigate the fraud found that the 'key logging' Trojan was on the businessman's computer and not on the Bank of America's system. The bank refused to take responsibility for the loss on the grounds that its systems were not hacked into and that all appropriate measures had been taken to complete the transfer.

Although this case suggests that banks might have started to become less generous in compensating defrauded customers, it is important to bear in mind that this fraud involved online banking and not credit card transactions. Banks do well out of credit cards because of the merchant fee and the high interest rates charged. Any action that reduced the confidence of actual or potential customers would harm the business, so it makes sense to absorb losses from credit card fraud provided they are not excessive. On the other hand, it might be argued that there is little in the way of incremental profit that can be made from internet banking except for longer term efficiency gains, so it is not surprising perhaps that the banks might be somewhat less willing to provide compensation for internet banking fraud.

An example of the customer friendly attitude of credit card companies to consumers is provided by American Express, whose 'Fraud Protection Guarantee' (American Express, 2010) is explained as follows:
'If you're unlucky enough to be a victim of fraud, it's our job to take care of it. You won't be held responsible for fraudulent charges, as long as you have taken reasonable care with your account details and PIN. So you can relax and spend securely, anywhere in the world. The moment we are alerted to a fraud, our team will work to resolve any issues as soon as possible and return your account to normal. For example, we'll credit your account in full and arrange a replacement Card with a new and secure Card number."

Finally it should be noted that the US is working hard to combat organised internet banking fraud. As reported on 30th Sep 2010, 'A federal crackdown on automated clearing house and wire fraud has produced 37 arrests (McGlasson, 2010) of a money mule operation, part of what law enforcement is calling a sophisticated bank fraud scheme that used malware to siphon off millions of dollars from U.S. bank accounts'. As explained by Preet Bharara, the Manhattan U.S. Attorney, the criminals targeted businesses and other entities using a malware known as the "Zeus Trojan," (a type of keylogger malware that is designed to steal banking credentials). The penalties imposed were severe, involving prison sentences of up to 30 years and fines of $1,000,000. This investigation demonstrated the effectiveness of cooperation between the NYPD, FBI and the Secret Service.

3.3.2 UK

In essence, the legal environment in the UK is not dissimilar to that in the US although there have been some well documented court cases concerned with mis-selling as discussed below.

One immediate similarity is in the efforts made to investigate internet fraud. Similar to the '37 arrests - case' in USA, a group of 19 hackers who committed online fraud in the UK was tracked down by UK police on 29th Sep 2010. It is alleged that a gang of Eastern Europeans made £2 million a month from online accounts by stealing victims'

log-in details using sophisticated software (the Zeus Trojan programme, as used in the US case mentioned above) which can be bought for just £300 over the internet. The detectives believed that the fraudsters made £6 million in just three months[1]. Martin Muirhead, chairman of the Virtual Task Force, said: 'This is an excellent example of how to bring to bear the resources and expertise of multiple agencies and public / private organisations in the UK. This is pioneering work led by the Metropolitan Police Service." This reference is to a special unit the Metropolitan Police set up in 2009 (the Police Central e-crime Unit, PCeU) to execute the Association of Chief Police Officers (ACPO) e-crime strategy. Although there are questions as to the adequacy of the funding of this unit, it has clearly been successful in a number of instances, such as the one mentioned above. It liaises closely with the National Cyber Forensics and Training Alliance (NCFTA) based in Pittsburgh USA particularly in tackling international e-crime[2].

On 1st April 2007, the 2006 Fraud Act came into force. This stipulated that banks and financial institutions should now become the first point of contact for cheque, plastic card and online fraud offences rather than the police. This passed the responsibility for collecting fraudulent information to these financial institutions which were then required to pass this on to the police. Critics of the law change focused on the lack of investigative criminal experience of the bank staff and the real possibility that banks involved in misconduct would hide the true facts and also might wish to hide the true extent of any fraudulent activity.

In terms of the willingness of UK banks to reimburse fraudulent transactions, it is difficult to draw hard and fast comparisons with the US. However, rule no.6 of the NatWest online banking terms and conditions (Natwest Online Banking) states: 'Where a transaction on the account is confirmed by use of the Security Details and the Service but you subsequently show that the transaction was not authorised by you, you will not be liable for that transaction provided you have kept your Security Details secret, you have acted with reasonable care and in accordance with these Terms and

[1] Gill, C. 2010. Hi-tech crime police quiz 19 people over internet bank scam that netted hackers up to £20m from British accounts, (accessed on 06/10/2010) http://www.dailymail.co.uk/news/article-1316022/Nineteen-arrested-online-bank-raid-netted-20m.html
[2] http://www.met.police.uk/pceu/national_crime_programme.html (accessed on 22/12/2010)

Conditions, and you have not acted fraudulently. Whether this would have resulted in the customer being reimbursed if a similar situation arose to the Bank of America case discussed in the last section is open to question, but superficially it would seem that NatWest is prepared to offer the customer more protection provided they adhere to the terms and conditions (the moral hazard implications of this are discussed on page 177). One of the people interviewed in the fraud study in this dissertation described how, after experiencing a fraud, they were interviewed by NatWest customer officers by phone, which was followed by the receipt of a mailing in the form of a personal declaration, following completion of which the fraudulent transaction was written off.

One further aspect of the legal environment in the UK is the number of court cases that have arisen on the basis of claims of mis-selling, particularly of PPI (Payment Protection Insurance). In October 2009, the Financial Services Authority ordered the reopening of around 185,000 rejected PPI mis-selling cases, following a County Court ruling in favour of Lynne Thorius, who had a £8,686 debt quashed on the basis of a mis-sold PPI policy. Other actions have been brought on the basis that credit card companies failed to abide by the Consumer Credit Act 1974 (subsequently replaced by the CCA 2006) on the basis that terms and conditions were not adequately stipulated. Although there have been some successes (eg Yates vs MBNA 2009) in general the courts are not very sympathetic to consumers avoiding their debt responsibilities on the basis of technicalities.

Finally it should be mentioned that there are now prescribed limits on some charges to customers following minor breaches of the terms and conditions. For example, the maximum fee for a late payment is £12. Before this limit was imposed, some cards charged over twice this amount.

3.3.3 EU

In order to modernise the payment systems and encourage the community trades among the member countries in European Union, from the 27th January, 1997 (Mercado-Kierkegaard, 2007), the European Parliament passed a series of Directives to promote cross-border transfers, credit card payment and electronic commerce.

The latest Directive proposed by the European commission is also called the New Legal Framework. A few highlights were listed by Sylvia Mercado-Kierkegaard (2007), for example, the geographic scope is set to cover payments in any currency and it is proposed to open up the market to further competition, for example from the non-banking sector.

A set of rights and obligations of service users and providers have been established, including, for example, the description of the provider's obligations in the following terms: the payment service provider is obliged to ensure the security of its payment verification instrument, to refrain from sending unsolicited payment verification instruments and to provide the user with an appropriate means to make a notification of loss, theft or misappropriation and with the means to prove he has made such notification (Article 47) (Mercado-Kierkegaard, 2007).

Compared to the limited liability of $50 in the United States, the European Directive on payment services applies a limited liability of 150 euros to cardholders in dealing with fraudulent transactions which occurred before the card-holder notified the provider, unless the card holder had acted fraudulently or been proved to be negligent (Steennot, 2008).

3.3.4 China

As the biggest emerging market in recent decades, the financial industry in China, in particular the development of modern financial products and services, is still at the infancy stage. For example, the regulation of the credit card service which is in use currently was established in 1999 (Yang, 2010). From 1999 till now, the development of the credit card industry has been through two turning points, from early stage to booming period. Because the relevant legislation concerning e-transactions and card payments is quite fragmented and out-of-date, there is no consistency in the way that financial organizations and banks deal with disputes.

As learnt from the interviews with senior mangers inside the financial industry in China, the banks apply different standards in dealing with fraudulent transactions, in particular in the case of the required notification period (e.g. within 24 hours, 48 hours or 72 hours after the fraudulent transaction occurred), and the different levels of limited liability and different standards of data protection. It pays to read the credit card agreements carefully. As noted on page 257 (chapter 8), within the notification period there is a strong likelihood that the individual will be compensated, but beyond this period the matter is a question for negotiation between the customer and the bank. Little evidence could be found where the notification period had been legally tested.

As discussed by H.F.Shi (2009), defrauded customers are not only advised to report any suspicious transaction or incidents to their banks in the first instance, but also to contact local police force as soon as possible. Basically, the punishment for card fraud offences is the same as for theft offences in China, e.g. Police would accept the fraudulent case and start the legal process if the monetary loss involved had reached RMB 1000 (about £100). Unfortunately, it is difficult to estimate the real loss caused by card fraud because the consequential loss of personal banking information can seriously aggravate the problem, so arguably the punishment should take this into account rather than the problem just being treated as simple theft.

On the other hand, as supported by the data analysis in the later chapters, banks in China are much less supportive to customers than the banks in western countries when dealing with fraud cases. An unsatisfied respondent mentioned that he had to collect crucial evidence (including CCTV footage) by himself in order to get a full refund from his bank. Further details of types of fraudulent transactions in China are given in chapter 7, section 7.2.4.

The lack of standardisation in dealing with fraudulent cases is exemplified in the differing terms and conditions attaching to credit cards in China. To investigate this, terms and conditions were obtained for five of the leading Chinese financial institutions, including the big four state owned banks. These were analysed to determine the degree of clarity attaching to five different categories, namely ‘general conditions’, ‘fees and charges’, ‘card use’, ‘liability of cardholder’ and ‘fraud and

protection'. The overview is presented in the following table (note that NC denotes 'not clear' and E denotes 'explicit').

Table 3.1 Clarity of credit card terms and conditions

	BOC	**ICBC**	**ABOC**	**CCB**	**CMB**
General conditions	NC	E	NC	E	E
Fees and charges	NC	E	NC	E	E
Card use	E	E	E	E	E
Liability of cardholder	NC	E	NC	E	E
Fraud and protection	NC	NC	NC	E	E

BOC (Bank of China); ICBC (Industrial and Commercial Bank of China); ABOC (Agricultural Bank of China); CCB (China Construction Bank);
CMB (China Merchants bank).

NC= not clear; E= explicit.

From the 'Liability of cardholder' row in the table above, we found that three of the five banks gave clear instructions requiring their customers to protect their personal information and sensitive banking details from others, e.g. 'do not release PIN or password to a third party'; 'do not lend bank cards to anybody else'. The other two banks did not provide detailed instructions, a typical case being ABOC, for which the printed version of the terms and conditions barely reaches two pages, and these contain very limited information.

In the 'fraud and protection' row, only two banks emphasise that customers should directly report any suspicious transaction to the bank service hotline. Also, those two banks promise that customers would get full support from the banks in dealing with credit card fraud if the customers reach all the requirements in the terms and conditions. The other three banks do not mention much information about fraud and protection in the printed version of the terms and conditions. As we discussed in chapter 7, the current situation of credit card services in China is neither standardized nor, in many cases, clearly stated. The inexperienced financial organizations are still trying to seek practical and effective ways of doing business with immature consumers. Were the incidence of financial fraud not low, then the lack of clarity

could provide a chaotic situation with considerable amounts of litigation involved in sorting out where liability should fall in the event of fraud. If the experience of the Western economies is any guide, then fraudulent activity is set to increase and the Chinese institutions would be well advised to clarify the legal basis of credit and debit card liability.

3.4 Conclusion

Both western financial organizations and emerging markets in Asia are facing similar challenges regarding financial fraud, in particular involving card payments and e-transactions. However, against this background, electronic transactions still represent the future because of their low cost, speed, convenience and high efficiency.

Although it might be assumed that the banks and credit card companies aim to eliminate all fraud, the cost of achieving this is likely to be prohibitive (even assuming that such a goal is achievable). This raises the question of the extent to which, at any one point in time, there is an equilibrium level of fraud which equates the marginal loss from fraud against the marginal cost of prevention. In other words, is there (in a financial sense) a level of fraud that is acceptable a particular bank or credit card company, and if so, how is it determined?

On a similar note, but at the macro level, there is the question of how far the legal system should favour the individual over the financial organisation, and to what extent the financial organisation should be regulated to provide a service that it deemed to be fair to all parties, rather than relying on the free market to do this job? On the international level, because the use of credit cards and online financial transactions transcends national boundaries, it is important that there is a basic level of uniformity otherwise this could lead to serious difficulties both in terms of settling transactions and in terms of resolving disputes. Although transnational organisations such as Visa, Maestro and Mastercard do transcend these boundaries, there is still some way to go to achieve a level playing field both in terms of legal uniformity and in terms of regulation.

Chapter 4 Bank Cards Transactions

4.1 Introduction

This chapter builds on the online security issues raised in the previous chapter but is focused particularly on the issues surrounding credit and debit card transactions, which form the basis for the fieldwork in chapters 6 and 8.

4.2 Credit & debit card transactions

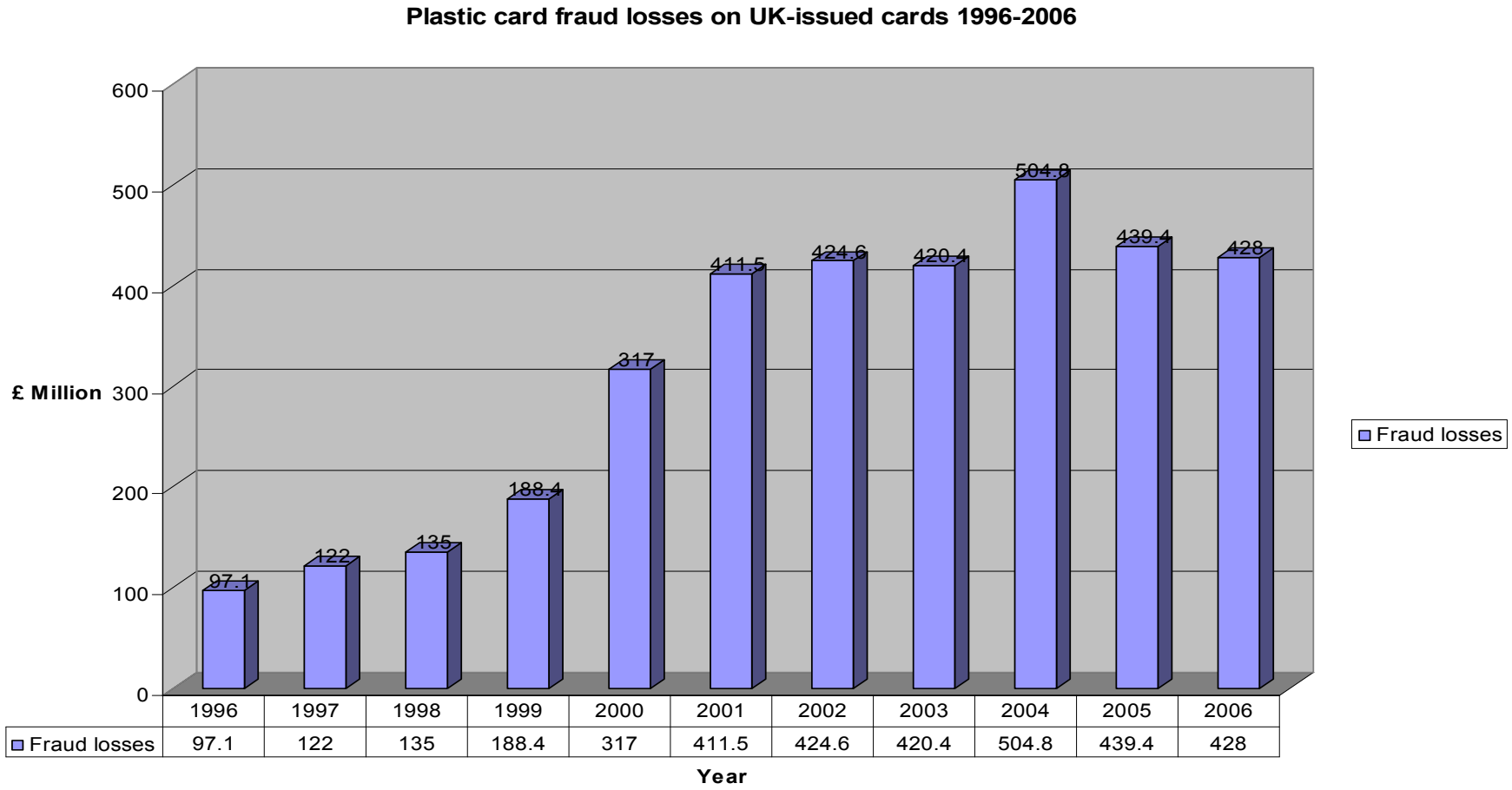
4.2.1 Overview

Credit cards have many advantages (Ritzer 1995,p4). On the one hand they can be used to increase consumers' spending power in the short-term, but in addition they provide tremendous convenience in that we can use credit cards 24/7 to purchase products we want by mail, telephone or internet; they can be used for cross-border transactions while cash cannot; they generate a transaction record that can help consumers in disputes with merchants; they provide a 'draw-down' facility in which interest is only paid on the outstanding balance (unlike a loan, where interest is fixed for the term) and they can help consumers to go through temporary financial difficulties, etc. Furthermore, it is easier to get a credit card than a personal loan, which involves lots of paperwork and interviews with banks. Customers can pay off a credit card balance at any time, while a personal loan has a fixed term for repayment, and early pay-off might incur an extra charge.

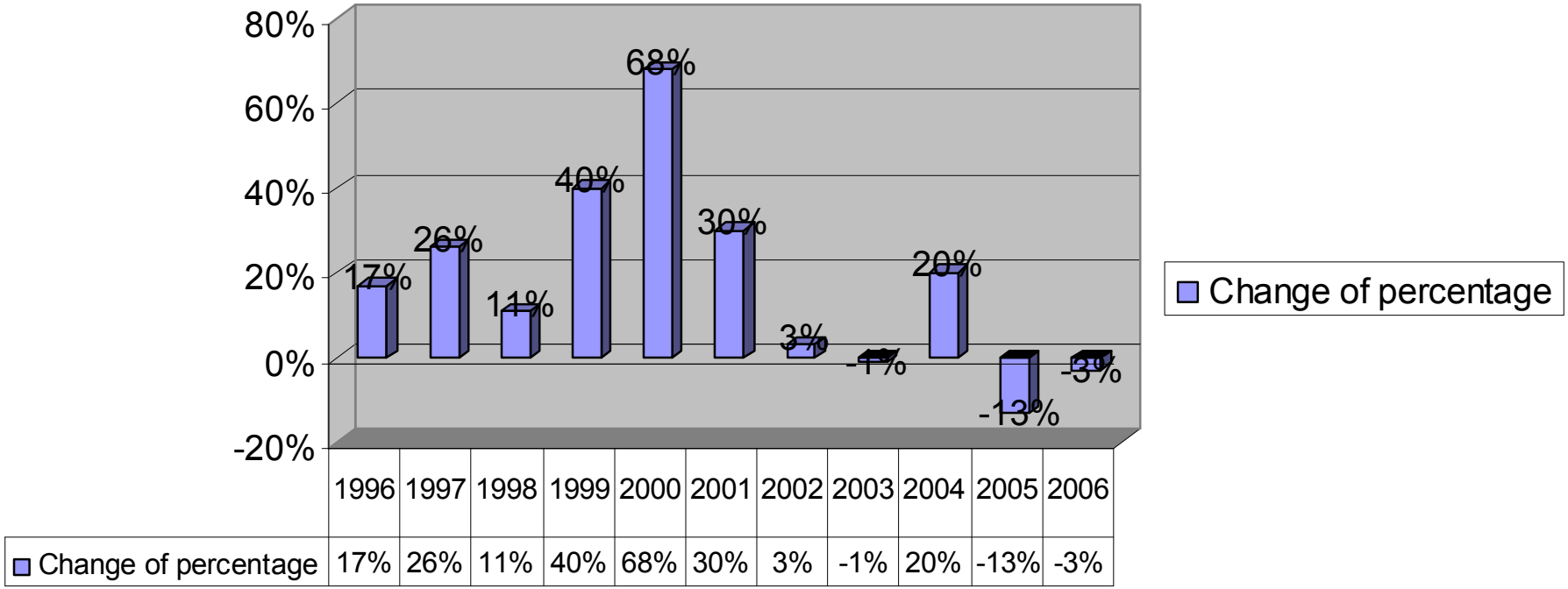
Compared to cash, credit cards are very convenient and safe to carry (Ritzer 1995,p4), and might help to reduce crimes directly against individuals. However, online fraud is a different matter – online credit card fraud involves intelligent criminal gangs and IT technologies. With the internet, fraudsters can potentially defraud many victims at low cost.

With plastic cards increasing in popularity, card fraud losses have increased considerably since 1996, growing from £97.1 million in 1996 to £439.4 million in 2005. From 2004 to 2005, the loss decreased by 13% because of the widespread use of Chip and PIN in the UK

(APACS 2006; APACS 2007). These reported losses are a combination of 'card present' and 'card-not-present' transactions. To a large extent, Chip and PIN has eliminated 'card-present' fraud, except where cards are presented in a jurisdiction where Chip-and-PIN is not used (e.g. USA).



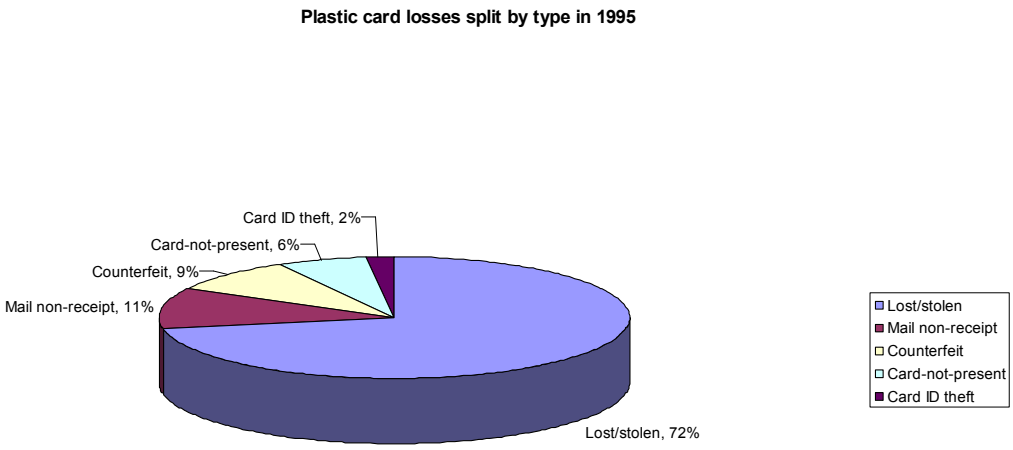
(source: APACS (2007))
Figure 4.1 Plastic card fraud losses on UK-issued cards 1996-2006



(source: APACS (2007))

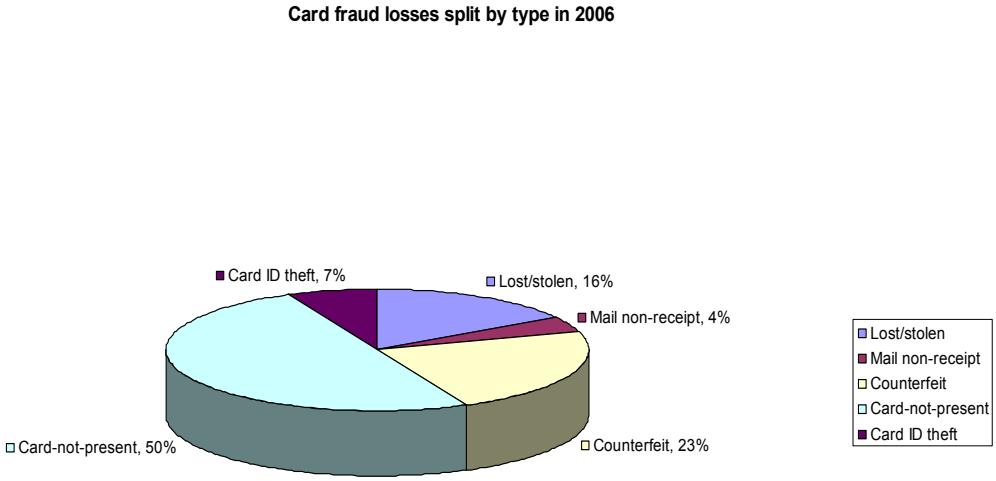
Figure 4.2 Change of percentage of plastic card fraud losses on UK-issued cards 1996-2006

The following figures show the plastic card losses split by different types of fraudulent transactions in 1995 and 2006 (APACS 2007).



(Source: APACS (2006))

Figure 4.3 Plastic card losses split by type in 1995



(Source: APACS (2007))

Figure 4.4 Card fraud losses split by type in 2006

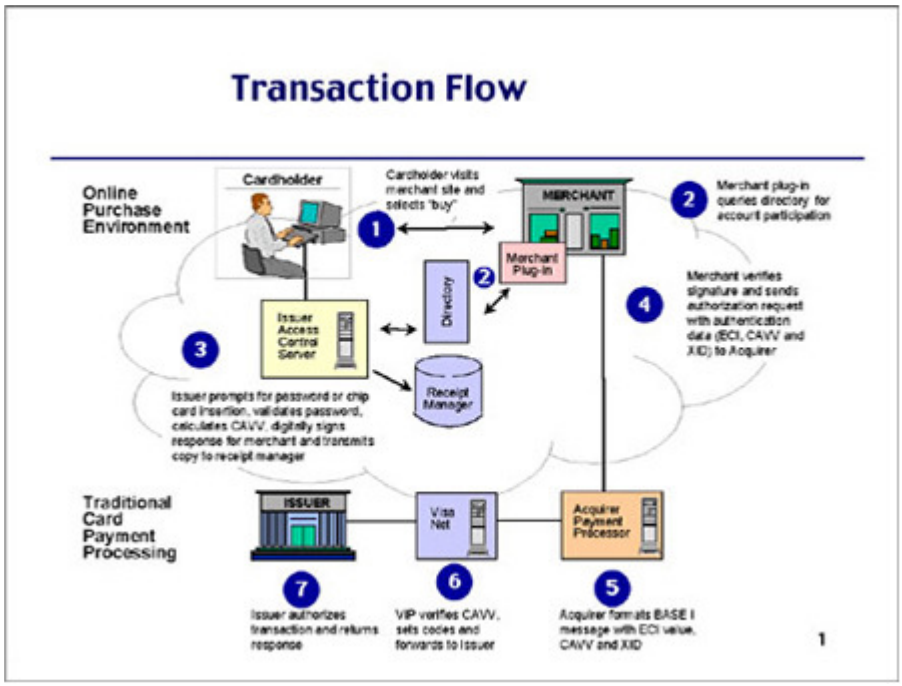
Table 4.1 Different types of plastic card losses
(Source: APACS (2006; 2007))

Different types of plastic card losses	Percentage (%)		
	1995	**2006**	**change**
Lost/stolen	72%	16%	-56%
Mail non-receipt	11%	4%	-7%
Counterfeit	9%	23%	14%
Card-not-present	6%	50%	44%
Card ID theft	2%	7%	5%

4.2.2 Visa process online

In this section we look more closely at the online purchasing environment to examine the vulnerabilities in each stage of the process. Figure 4.5 depicts the transaction flows involved in online purchases using a VISA credit card, together with each party involved in the transaction. Stage (1), (2), (3) and (4) describes how online transactions work using the example of online shopping. Stage (5), (6) and (7) describes the traditional card payment process which is sometimes described as a "Brick and Mortar" transaction.

The key feature of online financial transactions is that the whole transaction process can be conducted online using information technology without involving any staff from the branch. The obvious advantages for customers to use online financial services are: more convenient service access and provision, time saving, faster service response and personal circumstances (Walker, Johnson 2006). Besides these advantages for customers, banks also enjoy great benefits in offering internet banking, such as reduced costs and increased revenue growth from a potentially enhanced customer base. A survey conducted by Booz, Allen and Hamilton (Nehmzow 1996) showed that different banking channels have significantly different costs. Compared to the main delivery channels, online transaction costs are estimated to be only about 1% of branch banking costs.



(source : VISA)
Figure 4.5 Visa transaction flow

(1) Cardholder visits a merchant site and selects "buy."

(2) The merchant plug-in queries the directory for account participation.

(3) The issuer prompts for a password or chip card insertion, validates the password, calculates CAVV (Cardholder Authentication Verification Value (Authorize.Net), digitally signs response for merchant, and transmits a copy to the receipt manager.

(4) The merchant verifies the cardholder's signature, and sends an Authorization Request with Authentication Data (ECI(Merchant Account Blog), CAVV, and XIO) to the acquirer.

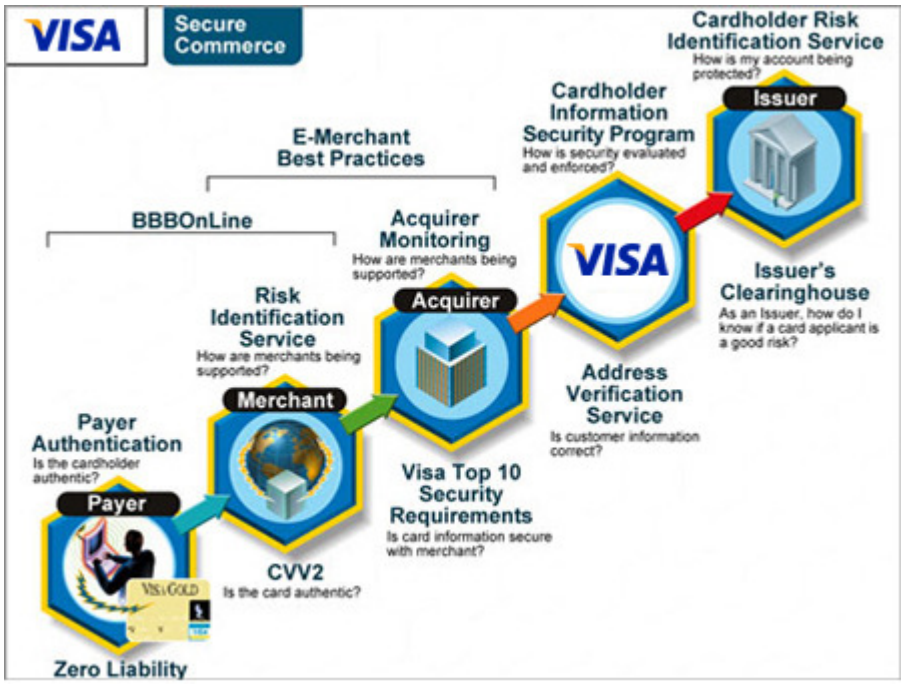
(5) The acquirer formats BASE II(BASE II) message with the ECI value, CAVV, and XIO.

(6) VIP (Visa Integrated Payment Platform) verifies CAVV, sets codes, and forwards to the issuer.

(7) The issuer authorizes the transaction and returns the response.

For more accurate description, payment processing on the internet is similar to the payment made offline. But there is one significant characteristic of online transaction: the card is not presented to the merchants on the internet. This characteristic makes online transaction very vulnerable to internet crime. Card-not-present (CNP) fraud

involves the use of stolen card details in the non face-to-face transactions either on the internet, by phone or by mail order (APACS 2006). It has been the largest type of card fraud in the UK for the past three years which caused the total loss of £183.2m in 2005 (up 21%). Because neither the card nor the cardholder is present when the transaction takes place, the difficulties in stopping this type of fraud hinges on three factors: for online businesses, the merchants are unable to check if the card is genuine. Without a signature or PIN, the merchants cannot satisfy the requisite verification procedures to ensure that they will be paid by the credit card company (irrespective of whether or not the person making the transaction is genuine or not). For card issuers, they cannot guarantee that the card information entered online is provided by the genuine cardholder.



(source: VISA)
Figure 4.6 Visa secure commerce

Visa Secure Commerce(VISA) includes a series of initiatives:

- Is the cardholder authentic? (Payer Authentication Zero Liability)
- Is the card authentic? (Risk Identification Service and CVV2
- How are the merchants being supported? (Acquirer Monitoring)
- Is the card information secure with the merchant? (Visa Top 10 Security Requirements)

- How is security evaluated and enforced? (Cardholder Information Security Program)
- Is the customer information correct? (Address Verification Service)
- How is the account being protected? (Cardholder Risk Identification Service)
- How do issuers know if an applicant is a good risk? (Issuer's Clearinghouse)

But for internet fraud, traditional password authentication on card not present transactions resulted in a sustained high level of fraud losses, estimated at £117.1 million in 2005 and £117.0 million in 2004 (APACS 2006). Customers need to provide their card information to affect a purchase on the internet. If the card is stolen, criminals have all the information required to make a transaction (ie the card number, security number, expiry date and card holder's name) because all the information is printed clearly on the card.

For the AVS/CSC(CardPaymentInfo), an automated cardholder address verification and card security code system is available for businesses that accept card-not-present transactions. This system allows merchants to verify the billing address of a cardholder and cross-check the security code when a transaction takes place without physical appearance of the card and cardholder (as the billing address does not appear on the card mere possession of the card does not provide all the information required to make a transaction). These checks provide additional information to protect both merchants and original card holders from fraud. Merchants can find out the suspicious orders in advance and stop the transaction on time. The assurance given by this system is potentially greater where the customer's delivery and billing addresses coincide.

4.3 Credit and debit card fraud

4.3.1 Overview

The following table gives an overview of the extent of fraudulent plastic card transactions for UK issued cards for the period 1997 to 2006. The only fraud to have grown at a spectacular rate throughout this period is card-not-present fraud. Other

frauds have had a period of growth followed by a period of decline as new technologies or procedures have been introduced to combat the fraud. The following sections look at each of the types of fraud to analyse both the activity and the steps that have been taken to try to control it.

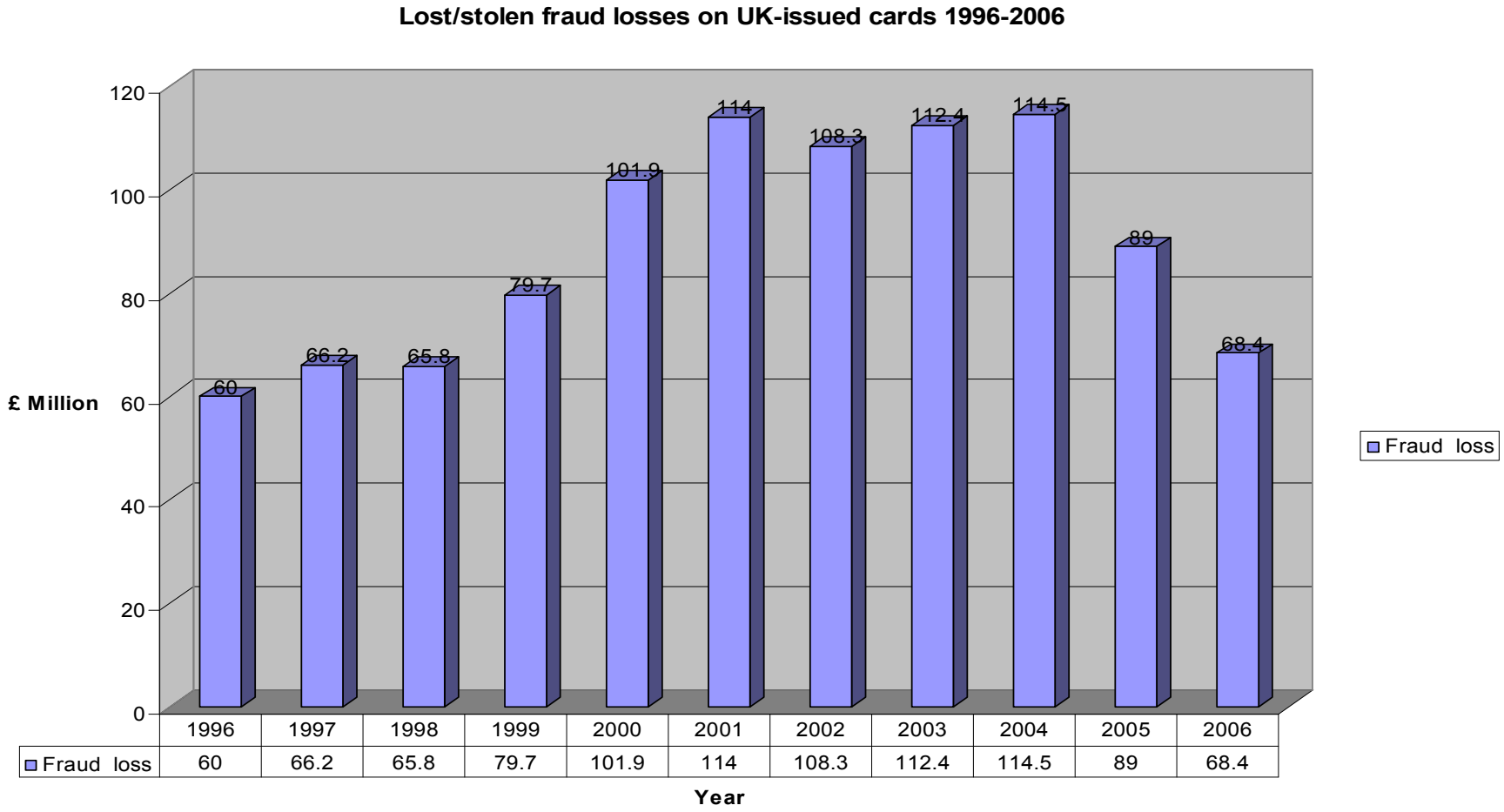
Table 4.2 Annual plastic card fraud losses on UK-issued cards 1997-2006
(Source: APACS (2007))

Annual plastic card fraud losses on UK-issued cards 1997-2006
All figures in £ millions

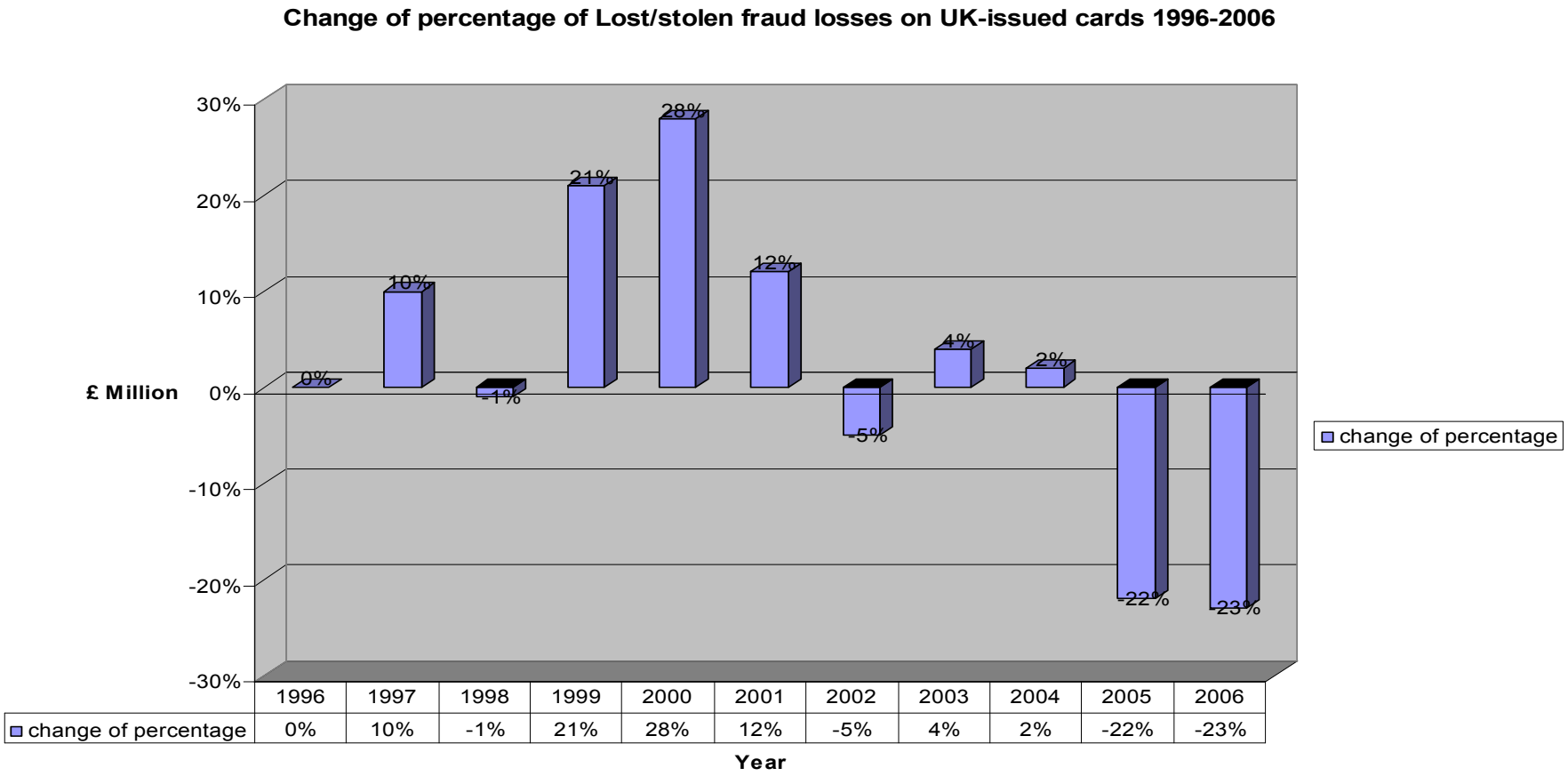
Fraud type	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Card-not-present	10.0	13.6	29.3	72.9	95.7	110.1	122.1	150.8	183.2	212.6
Counterfeit	20.3	26.8	50.3	107.1	160.4	148.5	110.6	129.7	96.8	99.6
Lost/stolen	66.2	65.8	79.7	101.9	114.0	108.3	112.4	114.5	89.0	68.4
Mail non-receipt	12.5	12.0	14.6	17.7	26.8	37.1	45.1	72.9	40.0	15.4
Card ID theft	13.1	16.8	14.4	17.4	14.6	20.6	30.2	36.9	30.5	31.9
Total	122.0	135.0	188.4	317.0	411.5	424.6	420.4	504.8	439.4	428.0
Contained within this total										
UK retailer (face-to-face)	72.2	74.8	93.0	139.1	188.9	186.9	177.9	218.8	135.9	72.1
Domestic/international split of total losses										
UK fraud	92.8	100.1	134.1	213.4	273.0	294.4	316.3	412.3	356.6	309.8
Fraud abroad	29.2	34.9	54.2	103.5	138.4	130.2	104.1	92.5	82.8	118.2

4.3.2 Lost/stolen

This type of fraud used to account for the largest losses of all types of card fraud. It mostly took place in shops without Chip and PIN equipment before the cardholders had reported the loss of the card. Before the introduction of Chip and PIN, merchants only relied on the signature of customers to check identification. It was very easy for criminals to forge the signature because the original signature had already been signed on the back of the card. Fortunately, lost/stolen card fraud has reduced 52% following the introduction of the Chip and PIN system (APACS 2007).



(source: APACS (2007))
Figure 4.7 Lost / stolen fraud losses on UK-issued cards 1996-2006

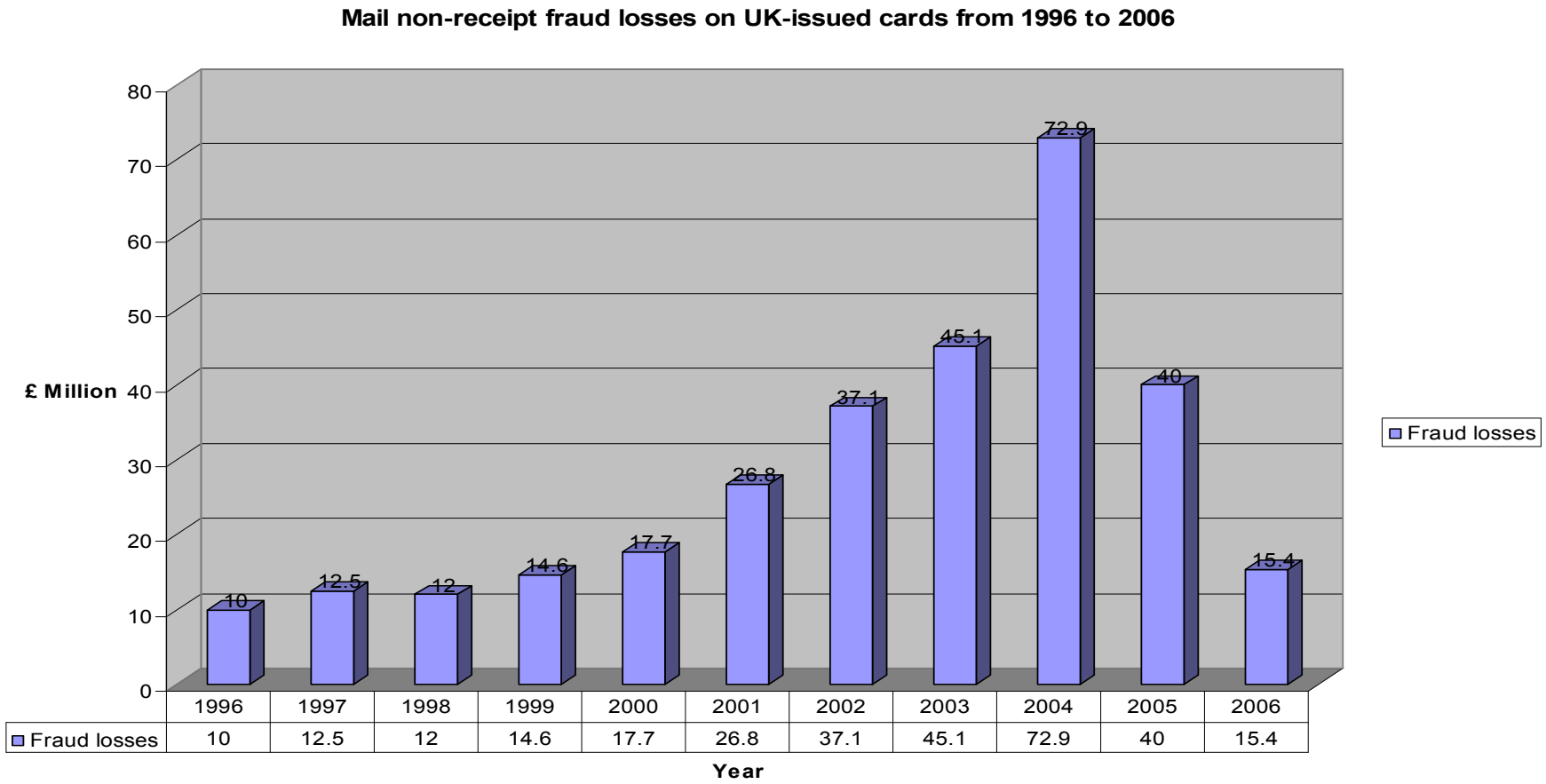


(source: APACS (2007))

Figure 4.8 Change of percentage of Lost / stolen fraud losses on UK-issued cards 1996-2006

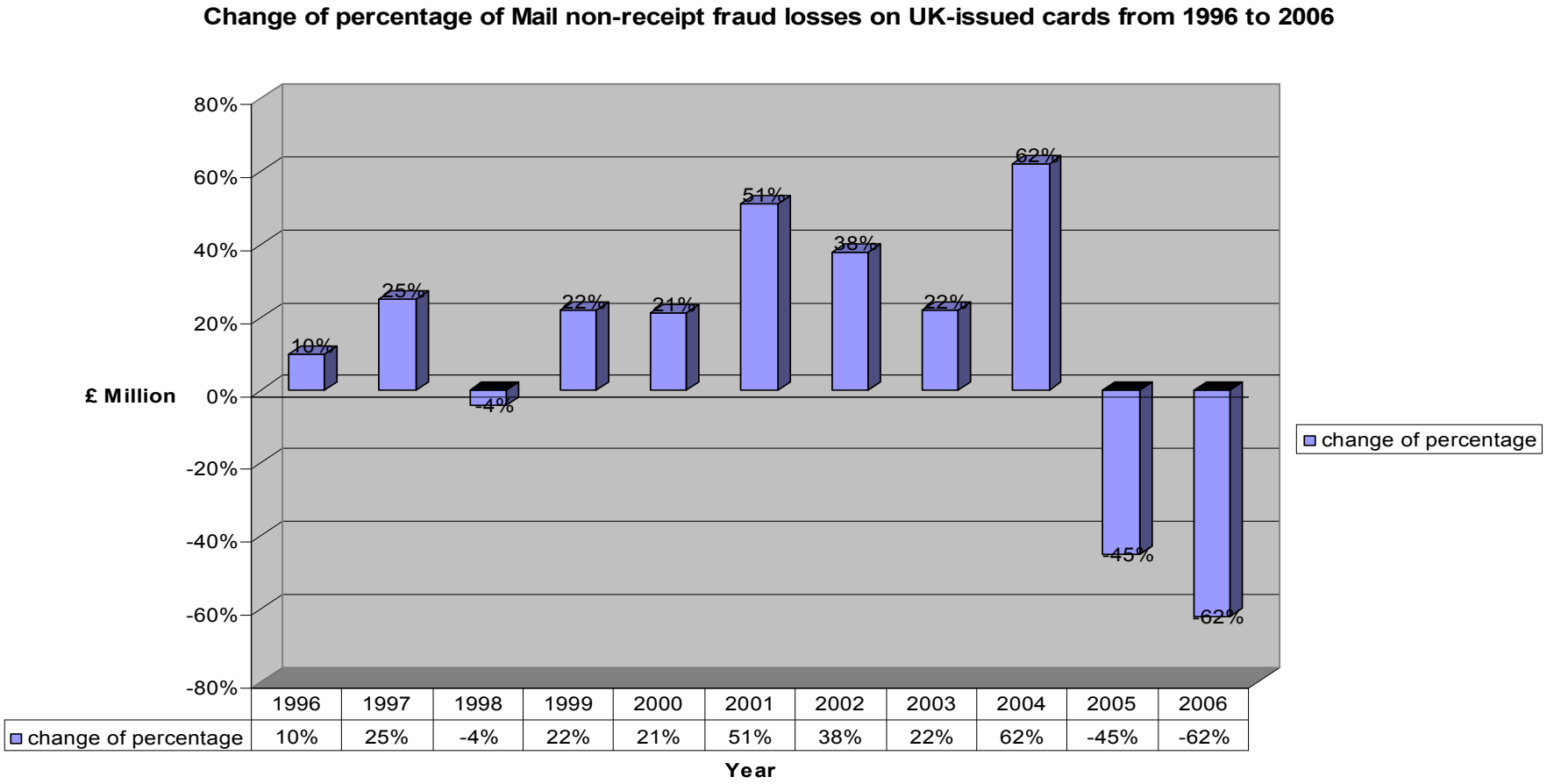
4.3.3 Mail non-receipt

This type of fraud involves postal systems, such as post office, postman and mail boxes. Those who steal from the postal system are lured by the fact that on any given day 500,000 unsigned credit cards are in the mail (Ritzer 1995,p86). Particularly at risk for this type of fraud are properties with communal letterboxes, such as flats and students halls of residents (APACS 2007). Alternatively, post-office insiders might collude with organized gangs to steal credit cards passing through the postal system. To combat this, a system of activation was introduced in 2005 requiring cards to be activated either by phone or online before they can be used, involving the cardholder giving the correct answer to various security questions. As can be seen from Figure 4.9 and Figure 4.10, this procedure had a dramatic effect on fraud from non-receipt of credit cards.



(source: APACS (2007))

Figure 4.9 Mail non-receipt fraud losses on UK-issued cards from 1996-2006



(source: APACS (2007))

Figure 4.10 Change of percentage of Mail non-receipt fraud losses on UK-issued cards from 1996-2006

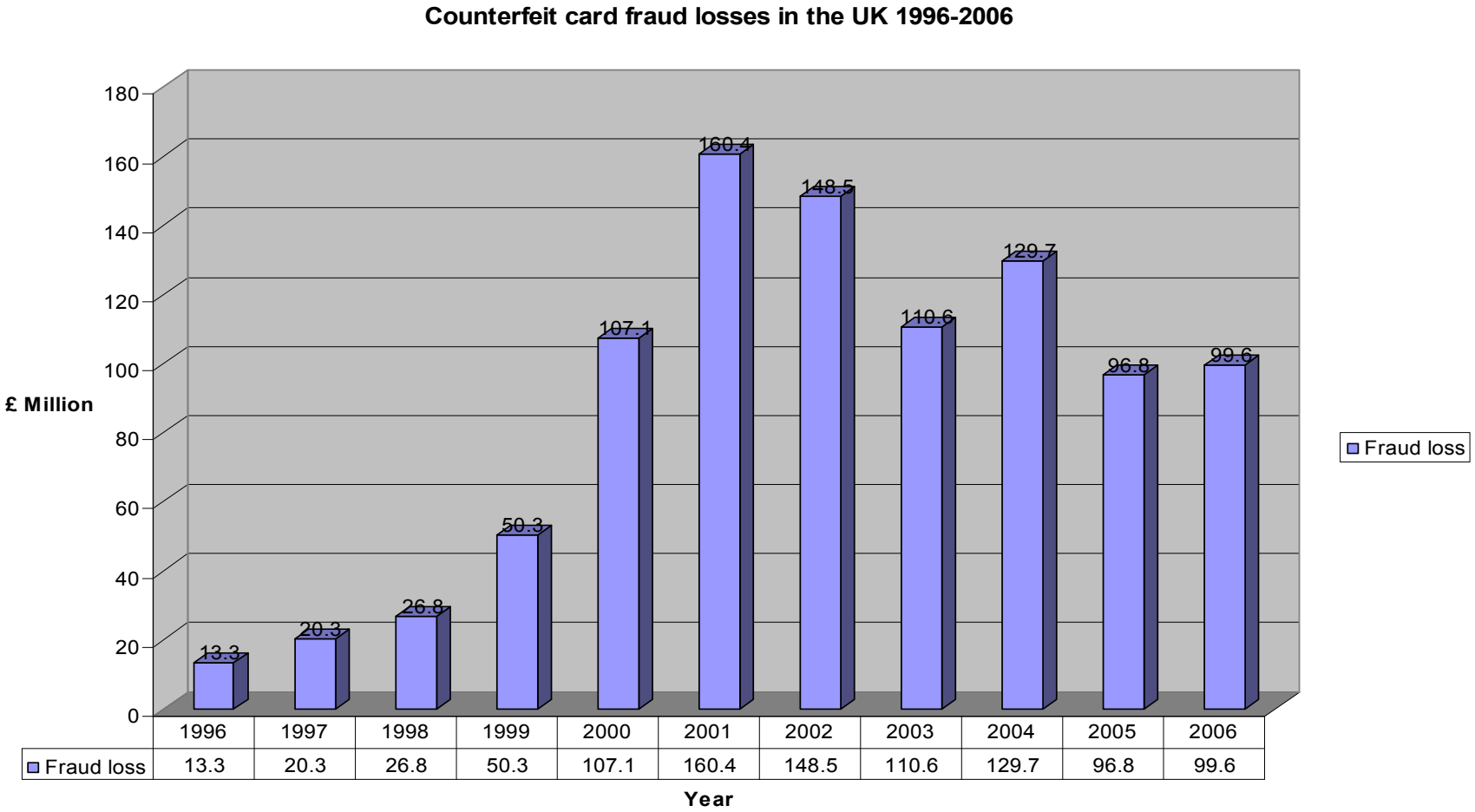
4.3.4 Counterfeit

Counterfeit card fraud occurs when an illegal copy of a genuine credit or debit card is made. Traditional bank cards carry account information using a magnetic stripe on the back, which can be copied electronically easily. Most counterfeit fraud involves skimming, which occurs when a corrupt employee copies the magnetic stripe of a customer's card electronically before handing it back, then sells the information to fraudsters to make clone cards. The introduction of chip technology has made this much more difficult to do, although in non-Chip-and-PIN environments, magnetic strip information might be sufficient to effect a transaction. This is well illustrated in Table 4.3 which shows the fraud losses from the cloning of UK cards to be declining in the UK (-8% in 2005/6) but increasing abroad (+51% in 2005/6).

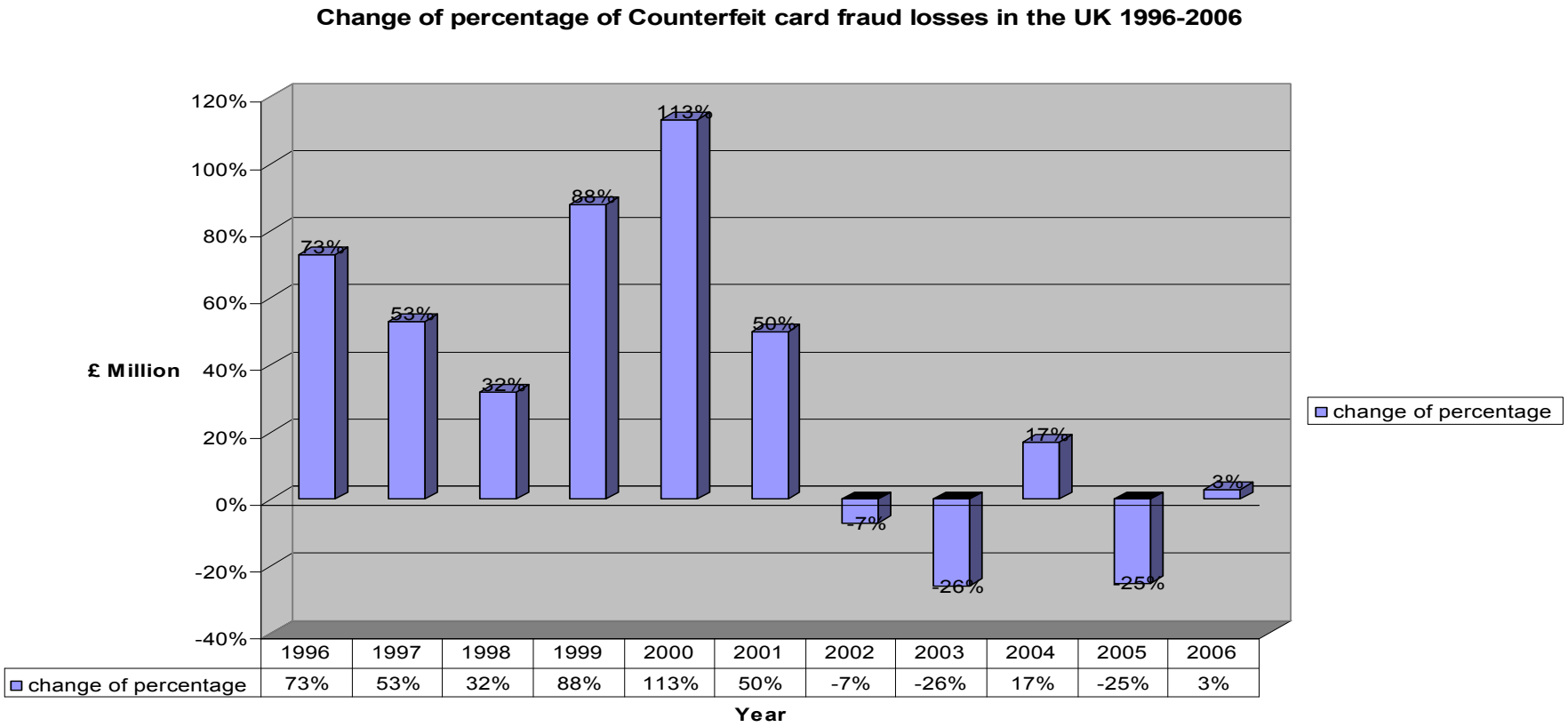
Table 4.3 Counterfeit card fraud losses in the UK and abroad 2004-2006
(Source from APACS (APACS 2007))

Counterfeit card fraud losses in the UK and abroad 2004-2006
All figures in £ millions

Region	2004	2005	2006	+/- change
Domestic (in the UK)	£105.9	£78.6	£72.1	-8%
Abroad	£23.8	£18.2	£27.5	+51%
Total	£129.7	£96.8	£99.6	+3%



(source: APACS (2007))
Figure 4.11 Counterfeit card fraud losses in the UK 1996-2006



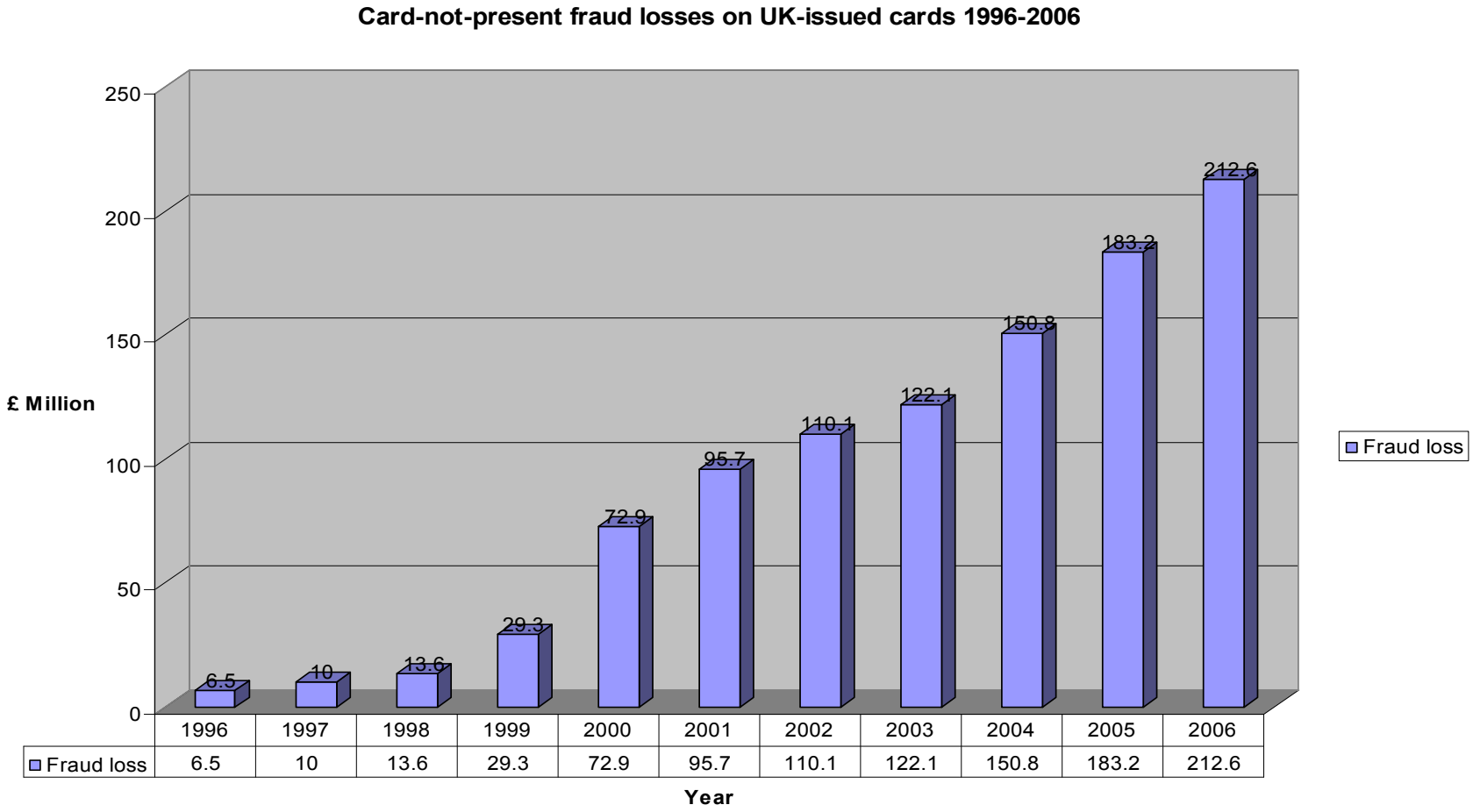
(source: APACS (2007))

Figure 4.12 Change of percentage of Counterfeit card fraud losses in the UK 1996-2006

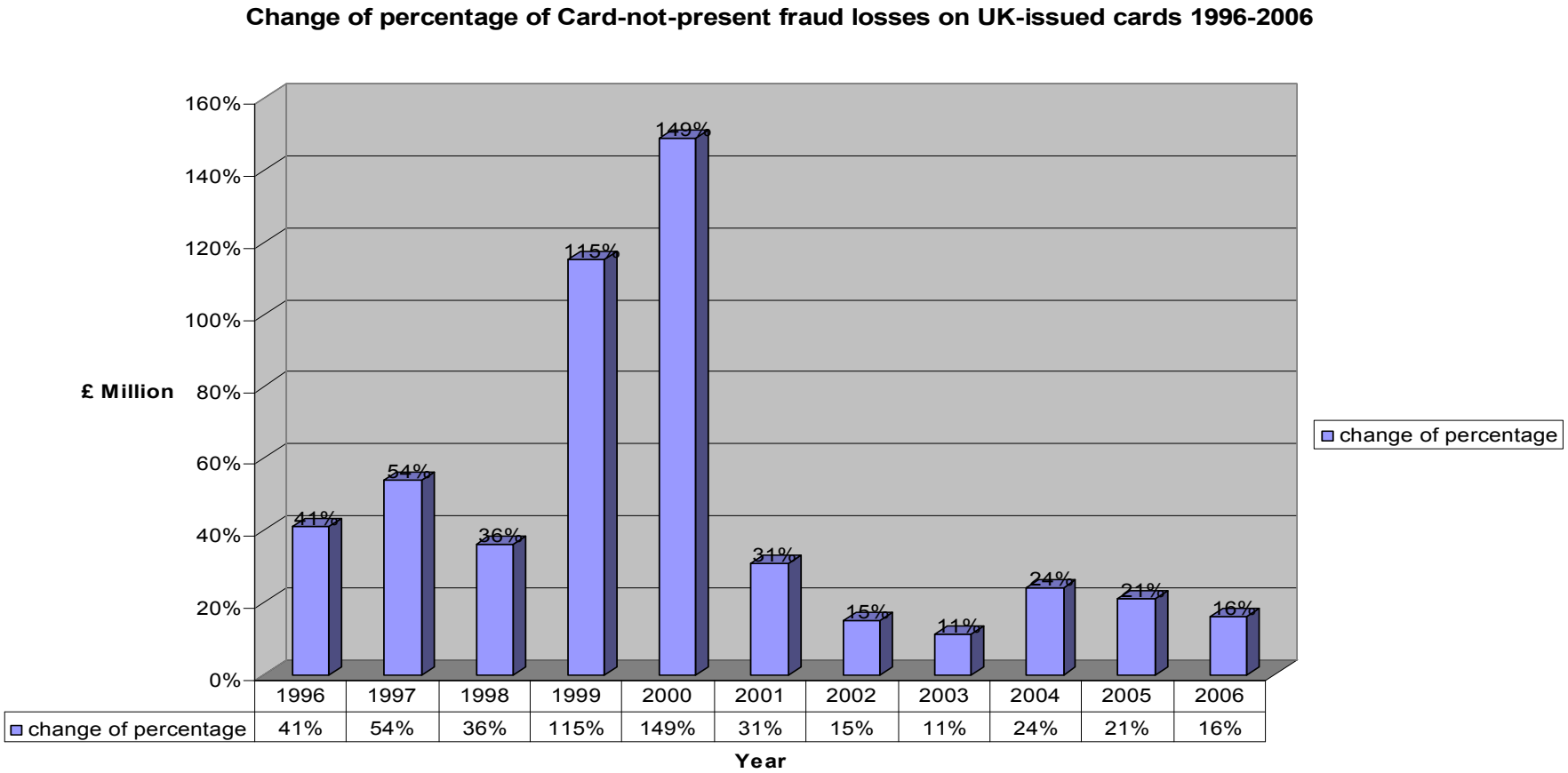
4.3.5 Card-not-present

Card-not-present (CNP) fraud involves the use of stolen card details in non face-to-face transactions either on the Internet, by phone or by mail order. It has been the largest type of card fraud in the UK for the past three years (APACS 2007). This fraud takes place when criminals steal authentic card details and use them to make purchase over the internet. The original card holders might not notice anything until they check their bank or credit card statements subsequently, or they are contacted by a suspicious credit card provider.

Compared to other types of fraud, card-not-present fraud is difficult to discover because neither the card nor the cardholder is visible to the vendor when the transaction happens. Online merchants are unable to check both the authentication of the card and the card holder to determine if they are genuine. Similarly, banks are unable to recognize whether the transaction is legitimate or not. Pattern of use checks have been introduced by most credit card issuers and more recently secure systems have been introduced such as Paypal and credit card verification procedures. These include NatWest Secure, MBNA Secure etc which require additional personal information to be required before a payment is processed. Banks are increasingly refusing card-not-present payments unless backed up with secure verification. Legal aspects of UK compensation are discussed in section 3.3.2.



(source: APACS (2007))
Figure 4.13 Card-not-present fraud losses on UK-issued cards 1996-2006

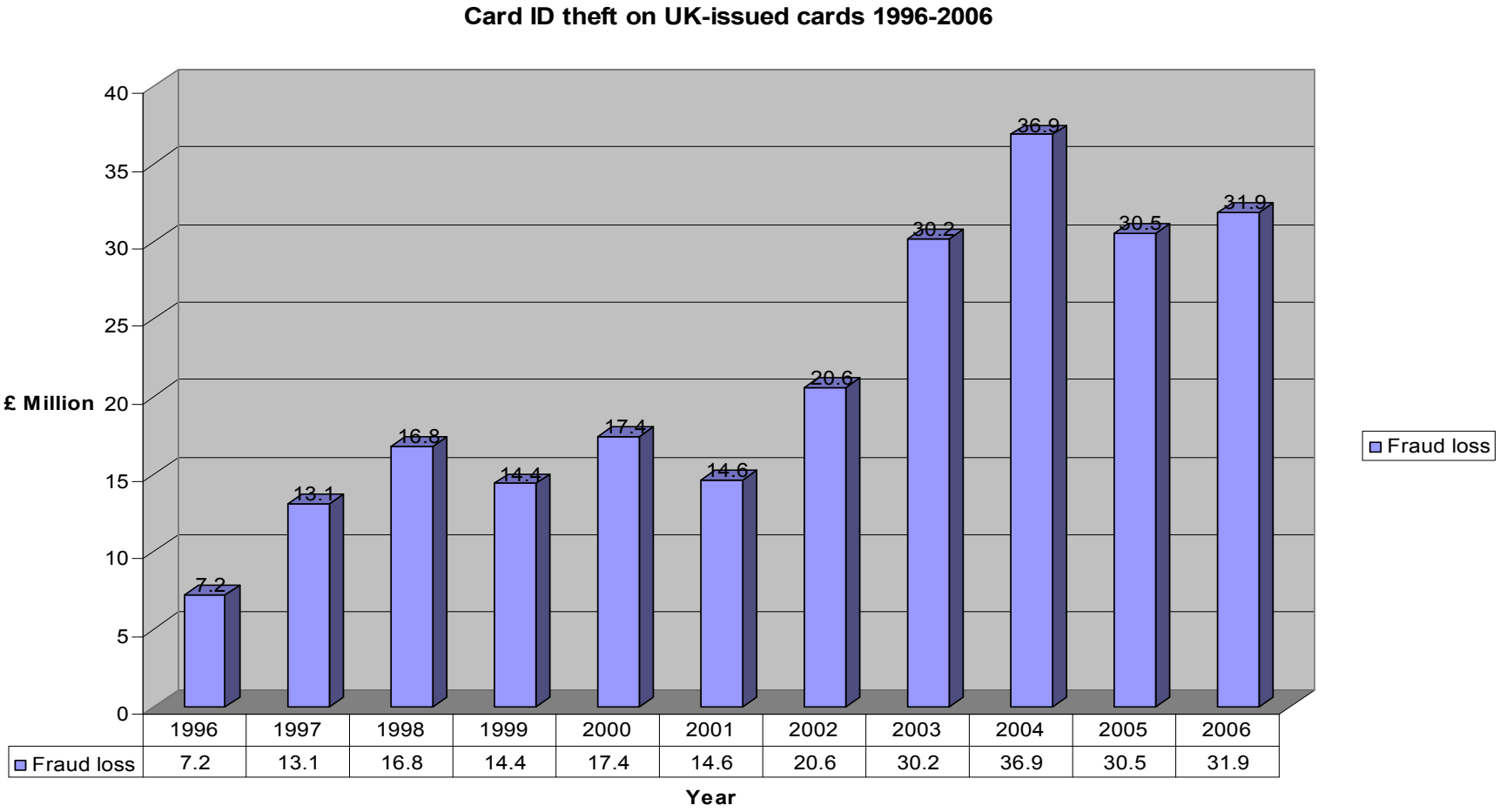


(source: APACS (2007))

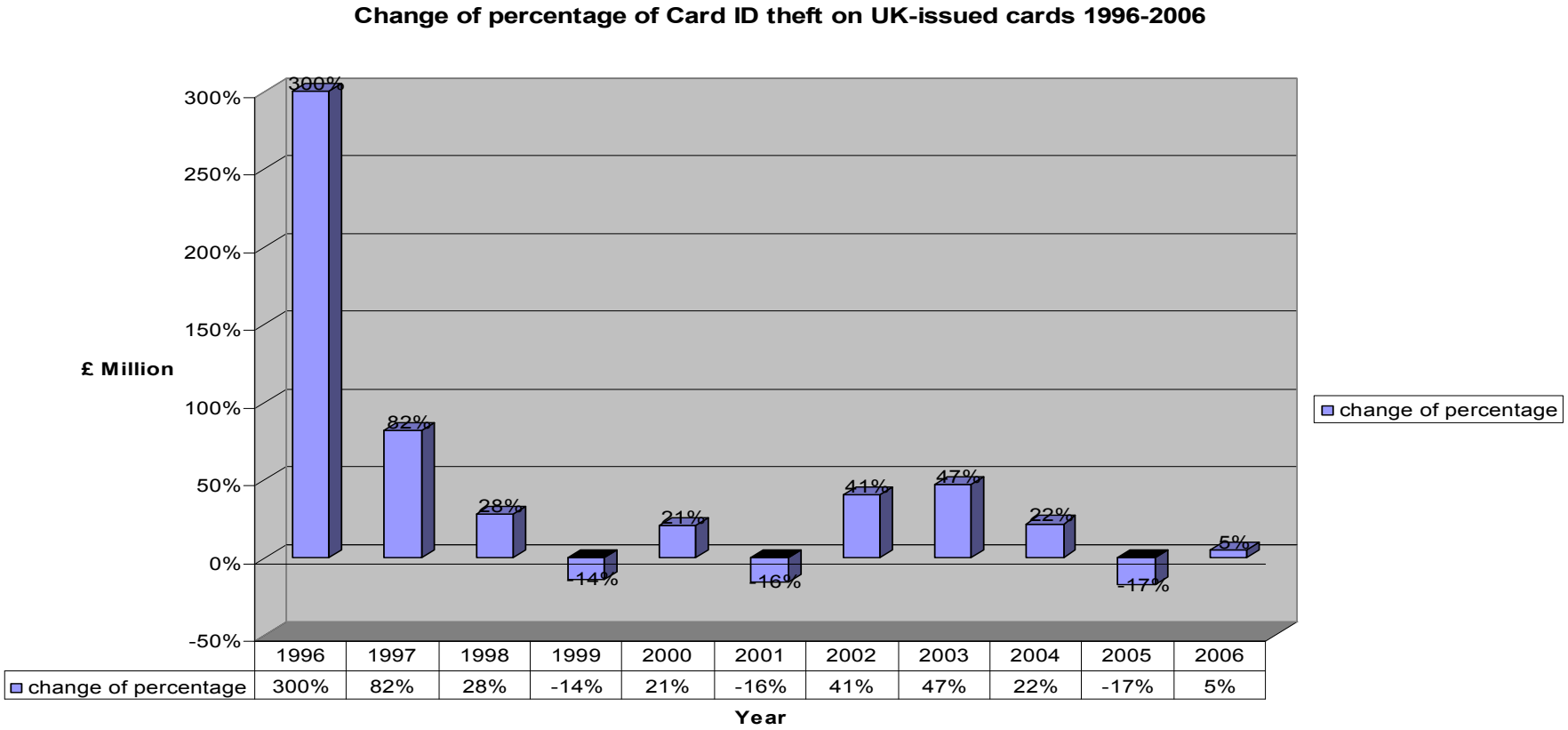
Figure 4.14 Change of percentage of Card-not-present fraud losses on UK-issued cards 1996-2006

4.3.6 Card ID theft

Even though a credit card remains safely in one's possession, fraud may still occur. For example, criminals can get card details by stealing bank statement or by a bin raids. Alternatively, criminals can co-operate with corrupt employees, such as hotel receptionists, store clerks and bank staff. For criminals with a high level of technical expertise, there is the possibility of attacking merchants' databases to get card information belonging to millions of customers. This information can be used for a variety of purposes, including card-not-present fraud, card cloning or sale of information on the Black Market – or possibly the issue of a new credit card to the fraudsters (Ritzer 1995,p89).



(source: APACS (2007))
Figure 4.15 Card ID theft on UK-issued cards 1996-2006



(source: APACS (2007))

Figure 4.16 Change of percentage of Card ID theft on UK-issued cards 1996-2006

4.3.7 Chip & PIN (definition, usage and vulnerability)

Chip and PIN has already been mentioned in the previous sections and the effect it had on reducing card-present fraud was noted. In this section we look more closely at the detail of the system and some of the problems associated with it.

Chip and PIN has changed the way we pay for 'card present' transactions in Europe but has still to be adopted in some major countries such as the US. Chip and PIN has been referred to as the biggest change in the means of payment since decimalization thirty-five years ago Anderson, R. *et al* (2006). In 1996, EMV (Europay international, MasterCard international and Visa international) created technology standards to enable the global introduction of Chip and PIN (Penn 2005). In the UK, from 1997 to 2003, several public trials were done in different locations. After years' preparation spent on the agreement between banks and retailers to shift the liability, before January 2006 more than 127 million Chip and PIN cards were issued and 80% of shops installed Chip and PIN equipment (2006). After 14 February 2006, more than 99.5% of all 'card present' transactions were verified by PIN, which reduced card fraud loss for the year 2006 by £65 million (2006).

The chip is a small piece of metal embedded in the card which stores card information in a form that is more secure than magnetic strip and is much harder to be cloned. As suggested by Search Security UK (Whatis.com 2008), a security-specific information resource for IT professionals in the UK, the card reader or POS can access the account information stored in the chip as soon as the Chip-and-PIN card is inserted. The PIN number (4-digit in the UK while 6-digit in China) entered by the card holder is checked against the information stored on the card. The transaction will be proved if the information matches.

UK is a leading country in adoption of Chip and PIN worldwide. Except for against fraud, there is a liability shift which benefits financial organizations. If a payment is fraudulent, liability for the fraud will go to issuers or acquirers and acquirer will pass the liability back to the merchant, if the merchant is not Chip and PIN enabled (Penn 2005). Here is the liability coming into force worldwide as following (Penn 2005):

Table 4.4 The proposed timeline of Chip-and-PIN application

01/01/2005	Europe
01/01/2006	CEMEA, Asia-Pacific, Latin America
01/01/2007	Rest of world
01/04/2010	Canada but not USA

More advanced Chip and PIN scheme called EMV, nearly all European countries are expected to implement EMV Chip and PIN over the next five years (Penn 2005). But in North America, things are totally different. USA is the country most resistant to adopt Chip and PIN (Penn 2005). The interesting point is that American banks are not as keen as European banks to shift liability to merchants and customers. For example, electronic banking is governed by 'Regulation E' which places the default liability squarely with the bank in the USA (Anderson *et al.* 2006). When disputes arisen in a transaction, banks either pay up or prove the fraud directly. Under the 'Regulation E', banks are willing to install security equipments and take other protective measures in USA.

On the other hand, weaknesses of Chip and PIN are emerging slowly. Firstly, both banks and merchants need to invest a large amount of money to install Chip and PIN system including software, hardware and staff training. For customers, we have to remember more and more numbers in daily life. If we have three cards in purse, we have to remember three four-digital pins because we are suggested to use different PIN for each card for security reasons.

At the moment in the UK, debit cards and credit cards are still keeping the mag-strip on the back of cards which still take the risk of being cloned. If we get rid of the mag-strip completely, cards issued in the UK can not be used in other countries. On the contrary, tourists will have problems to make payment in the UK using cards issued in their countries. Even in the UK, some merchants still reject to install Chip and PIN equipment and customers have to sign at the check out in a traditional way.

Some people say Chip and PIN changed the way we pay successfully and beat card fraud efficiently. Others think Chip and PIN doesn't sort out problems indeed and it is falling apart to some extent. The current challenge we face focus on the card-not-present fraud including transactions by internet, mail and telephone. Barclays, claims to be the first in the UK to offer a card based solution to cut online fraud, which in turn eliminates the need for tedious pass codes and memorable words (Barclays' smart approach to online fraud targets 0.5m customers. 2007/4). By the end of this year, more than half million customers will receive free Pins entry card readers. This is the latest security protection provided by Barclays'. Last year it offered free anti-virus software to its online banking customers (Barclays' smart approach to online fraud targets 0.5m customers. 2007/4).

4.4 Summary

Despite the problems of controlling fraud, the number of online banking customers in the UK more than doubled between 2002 and 2006 to 16.9 million, with almost half of internet users now banking online (Barclays' smart approach to online fraud targets 0.5m customers. 2007/4). This is despite a growing total of aggregate plastic card fraud which might be expected to erode confidence in the system. Analysis of the individual types of fraudulent activity shows an interesting picture, with a growth in a particular fraud being countered by a new technology that reduces the possibilities for fraudulent gain – a good example being the introduction of Chip and PIN in 2005 on card-present (or face-to-face) fraud. The area that seems to be most out of control is 'card-not-present' fraud, which has shown a persistent year-on-year growth throughout the 1997 to 2006 period.

The next chapter deals with the methodology of the field work which looks at the experience and perception of individuals.

Chapter 5 Methodology and Research Design

5.1 Introduction

In this chapter, we are discussing the methodology and research design of my study, concentrating in particular on the following aspects: (i) the philosophical underpinnings (interpretivist versus positivist), (ii) the quantitative and qualitative research approaches employed, (iii) the non-parametric statistical methodology used, and finally the data collection methods and data analysis methods adopted.

5.2. Interpretivist or positivist

Natural science as a rule adopts quantitative methods and follows the positivist approach, whereas social science tends to concentrate on qualitative methods and employs an interpretive approach. Positivist researchers believe that there is a reality existing out there and it is possible to quantify the reality. Researchers posit hypotheses and test these using appropriate data to determine whether or not they are supportable. It is important that the research activities don't change or influence the reality which is being studied.

The interpretive researchers doubt if there are fixed 'rules' out there and maintain that it is impossible to quantify the real world even it were to exist. They focus on understanding of the immediate problem in context instead of attempting to discover a general truth. For interpretive researchers, research activities (including the presence of researchers) can change or influence the phenomenon which is being studied. In the field of social science, a particular challenge is posed by the fact that the researcher is a member of society and is involved in the research environment, making neutral observation very difficult.

According to the statements made by William and Baiche (2001, p203), Auguste Comet, the nineteenth century French Philosopher, was the first to maintain that society could be analysed empirically just like other subjects of scientific inquiry. Since then, positivist social researchers have often applied the methodologies of natural science to the social sciences and have established well founded procedures of

analysis and interpretation (for example in the field of econometrics). Both positivist and interpretivist approaches are currently in use in the social science field.

The research methodology of this study relies on the positivist more than the interpretivist approaches because we are looking to establish general facts by testing hypotheses (such as those contained within the questions in the questionnaire) and using statistical methods. The overall research issue we focus on is the security of electronic financial transactions and internet fraud both in the UK and China – this thesis is an investigation into the various components of this problem. The key questions are the following: what types of internet fraud are related to electronic financial transactions; how serious is the effect caused by internet fraud; who are the individuals or organisations involved in the various aspects of the problem, and how can the risks of the internet fraud and online financial transactions be reduced?

5.3. Quantitative or qualitative research

As discussed in the previous section, quantitative research methods are generally associated with the positivist approach, while qualitative research methods are commonly associated with the interpretivist approach. The following table shows the main differences between quantitative and qualitative research methods (Bryman, Bell 2003, p302):

Table 5.1 The contrast of quantitative and qualitative research

Quantitative	**Qualitative**
Numbers	Words
Point of view of researcher	Points of view of participants
Research distant	Research close
Theory testing	Theory emergent
Static	Process
Structured	Unstructured
Generalization	Contextual understanding
Hard, reliable data	Rich, deep data
Macro	Micro
Behaviour	Meaning
Artificial settings	Natural settings

For example, numbers or words. Quantitative research focuses on numbers and usually applies mathematics and statistics to test hypotheses and to explain research results. Qualitative research on the other hand pays more attention to words (ie descriptive analysis). Words are used to present the analysis of social phenomena instead of numerical measurement. Bryman and Bell (2003, p302) stated: 'Quantitative researchers typically bring a set of concepts to bear on the research instruments being employed, so that theoretical work precedes the collection of data, whereas in qualitative research concepts and theoretical elaboration emerge out of data collection'.

5.4. Parametric and Non-parametric statistics

Parametric tests use the actual data values and the test itself specifies certain conditions about the parameters of the population from which the research sample was drawn (Siegel 1956). Non-parametric tests generally use a proxy for the actual data values (such as rank ordering) and make assumptions about the distribution of these proxy variables rather than the actual values of the distribution from which the sample was drawn. Non-parametric tests can be particularly useful where there are non-regularities in the distribution of data (eg large non-representative outliers) or where the distribution of the data is not known.

The reason for choosing non-parametric statistical tests in this study is because the assumptions required by parametric statistical test are violated due to characteristics of the data set, which will be discussed in detail in the following section. Siegel (1956, p31) listed the advantages of non-parametric statistics as follows:

(1) The accuracy of the probability statement does not depend on the shape of the population, although some nonparametric tests may assume identity of shape of two or more population distributions, and some others assume symmetrical population distributions.
(2) If sample size as small as N=6 are used, there is no alternative to using a nonparametric statistical test unless the nature of the population distribution is known exactly.

(3) There are suitable nonparametric statistical tests for treating samples made up of observations from several different populations.
(4) Nonparametric statistical tests are available to treat data which are inherently in ranks as well as data whose seemingly numerical scores have the strength of ranks.
(5) Nonparametric methods are available to treat data which are simply classificatory, i.e., are measured in a nominal scale.
(6) Nonparametric statistical tests are typically much easier to learn and to apply than are parametric tests.

5.4.1 Differences between variables

Healey (1993, p3) defined: 'a variable is any trait that can change values from case to case and the causes are called independent variables and the 'effects' or result variables are called dependent variables'. Interestingly, any given variable can be measured at more than one level (Kendrick 2005, p39). For example, the variable "age" can be measured as an exact number in a numerical format like 20, 32, 49, but we can also rank the variable "age" into groups and give them a ranking, eg: rank (1): 18 - 26,; rank (2): 27- 35; rank (3): 36-44.

Categorical variables are those variables for which data are gathered in response categories that have been set up or predetermined by the researcher (Kendrick 2005, p39). Researchers have categorised possible answers in advance and respondents only need to tick proper category containing their answers. The categories of variables need to cover all possibilities of the answers but not overlap with each other. Consequently, respondents can only find and choose one category which fits in their answers to the questions.

Now we look at two different types of categorical variables: nominal and ordinal. One example of nominal variable is "gender", which is measured in the categories of male and female. There is no rank order for these two categories and either of them can be rank 1 or 2. Ordinal variables are measured by categories which have hierarchy and order. For example, we use five scales to measure attitudes: strongly disagree; disagree; neither disagree nor agree; agree; strongly agree.

5.4.2 Non-parametric Tests

Most non-parametric tests work on the data which use higher score to label higher rank. Then the analysis is carried out with ranks instead of actual data used widely in parametric tests. Now we have a look at two popular tests below that were used in this study:

(1) Chi-square

Chi-square test is a non-parametric test and probably the most frequently used hypothesis test in the social sciences (Healey 1993, p254). Generally speaking, we need to set a null hypothesis under the assumption that the variables are independent. If we find little difference between the expected and observed frequencies, we would see no reason to reject the null hypothesis. On the other hand, if we are able to find statistically significant differences between the expected and observed frequencies, we would reject null hypothesis. As with all statistical tests, there is a chance that the null hypothesis might be rejected when it is actually correct (type I error) – this probability is captured in the level of significance, α, which is often set at 5%.

(2) Logistic analysis

Field, A. (2000, p164) gives the following definition 'logistic regression is multiple-regression but with an outcome variable that is a categorical dichotomy, and predictor variables that are continuous or categorical'. In this study, the dependent variable (outcome variable) has only two values, either 'fraud' (1) or 'no fraud' (0). This is regressed on a number of independent variables, such as age, gender and IT skills to gauge their influence in explaining the occurrence of fraudulent transactions online. Also, logistic analysis allows us to discover, through significance tests on the estimated coefficients, whether a certain variable has more significant performance than others, e.g. gender is playing a more effect role to explain the occurrence of fraudulent transactions on the internet.

5.5. Data collection methods

Various data collection methods were used depending on the nature of the research being carried out. It is common to combine more than one data collection methods to support the research results. We choose self-completion questionnaire and semi-structured interview as data collection methods. Data set collected by survey questionnaire were analysed quantitatively using SPSS and transcripts recorded qualitatively by semi-structured interview were used as additional evidence for this research.

5.5.1 Semi-structured interview

Bryman and Bell (2003) offered the following statements about semi-structured interview: 'the research has a list of questions or fairly specific topics to be covered (referred to as an interview guide), but the questions may not follow on exactly in the way outlined on the schedule and the questions not included in the guide may be asked'. In brief, the semi-structured interview is a flexible process based on the real-time interaction between interviewer and interviewee.

The ideal interviewees are the people who have experience of working in the financial industry both in the UK and China. We are expecting that they would like to share some information about the latest technology / policies / actions related to online financial transactions / internet fraud.

5.5.2 Self-completion questionnaire

The self-completion questionnaire is designed for respondents to read instruction and answer all the questions at their own pace. Bryman and Bell (2003, p141) also stated: "because there is no interviewer in the administration of the self-completion questionnaire, the research instrument has to be especially easy to follow and its questions have to be particularly easy to answer'.

The top advantages of the self-completion questionnaire are that it is cheaper to administer; easier to administer and is convenient for participants. But the main disadvantages of the self-completion questionnaire are the strong possibilities of missing data and lower response rates.

Several tips are provided by Bryman and Bell (2003, p146-150), eg: (1) Do not cramp the presentation; (2) provide a clear presentation; (3) use vertical or horizontal closed answers (4) provide clear instructions about how to respond; (5) keep the questions and answers together.

There are no golden rules for questionnaire design and what we can do is to improve questions and make them work better. However, adapted and suggested by Churchil and Gilbert (2002, p315) a well recommended procedure for developing a questionnaire consisted of nine steps:

Table 5.2 Procedure for developing a questionnaire

Step 1	Specify what information will be sought
	↓
Step 2	Determine type of questionnaire and method of administration
	↓
Step3	Determine content of individual questions
	↓
Step4	Determine form of response to each question
	↓
Step5	Determine wording of each question
	↓
Step6	Determine sequence of question
	↓
Step7	Determine physical characteristics of questionnaire
	↓
Step8	Re-examine steps 1-7 and revise if necessary
	↓
Step9	Pre-test questionnaire and revise if necessary

Step 1: Specify what information will be sought

In the very first step, researchers can use potential hypotheses as a checklist to determine what information will be collected and specify the research purpose.

Step 2: Determine type of questionnaire and method of administration

In the second step, we can decide whether to choose open-end questions or fixed options. Considering the cost and efficiency of administration, we opt to conduct the questionnaire study by post.

Step 3: Determine the content of individual questions

Based on the previous two steps, we can look at the content of the questionnaire at this stage and make further discussions, e.g. whether or not the content of questions is clear and applicable; whether or not the format of questions is clearly and efficient; if there any ethical issues involved.

Step 4: Determine the form of response to each question

Responses will be various relying on the different formats of questions used. Usually speaking, the open-ended questions can generate insightful replies using the respondent's own form of expression. But fixed-alternative questions make data recording and analysis convenient and efficient.

Step 5: Determine the wording of each question

It is crucial to choose the exact words / phrases to present questions to avoid ambiguity and misunderstanding. A few basic principles suggested by Churchill and Iacobucci (2002, p337-344) are: 'use simple words; avoid ambiguous word and questions; avoid leading questions; avoid implicit alternatives; avoid implicit assumptions; avoid generalizations and estimates and avoid double-barrelled questions'.

Step 6: Determine the sequence of question

Again, there is no certain rule to apply for the sequence of questions. Some surveys start with general questions, e.g. gender; age; education etc. Others would like to

begin with the key questions immediately, e.g. attitudes to internet banking; usage of online financial transactions etc.

Step 7: Determine physical characteristics of questionnaire
Presentation of survey questionnaire is crucial, in particular for mail questionnaires which need to be persuasive and attractive for a reasonable response rate and data quality. Also, the size of survey questionnaire is important. Generally speaking, small size works better than big size. However, there is no clear definition of 'small' and 'big'.

Step 8: Re-examination and revision of the questionnaire & Step 9: Pre-test the questionnaire
Use either peer-review or a small-scale trial as a test run to examine how a survey questionnaire performs in a relatively real environment. If the trial results are not close to expectations or throw up problems of misinterpretation or ambiguity, the researchers still have chance to improve the questionnaire and to make corrections.

5.6. Data analysis methods

SPSS for Windows is the most widely used package of computer software for doing quantitative analysis. SPSS was used to analyse the data collected using the postal survey questionnaire.

5.7. Research framework and hypotheses

In this section, we have a look at the framework model of my study and hypotheses. The framework is to show the structure of the study and the linkages between four sections of the survey questionnaire: basic financial information; IT usage information; personal information and optional section. Then the research hypotheses of my study are explained in relation to each section of the survey questionnaire.

5.7.1 The framework of the study

This framework explains the main aspects of this study and structure of the survey questionnaire used for data collection. The detailed discussion about the questionnaire is in the following section. In brief, we start to investigate and observe the fraud occurrence from four approaches: (1) basic financial information; (2) IT usage information; (3) personal information and (4) optional section to be competed only by defrauded individuals. In Figure 5.1, black arrows show the direction of predictions. The red arrows stand for the assumed connection between four approaches.

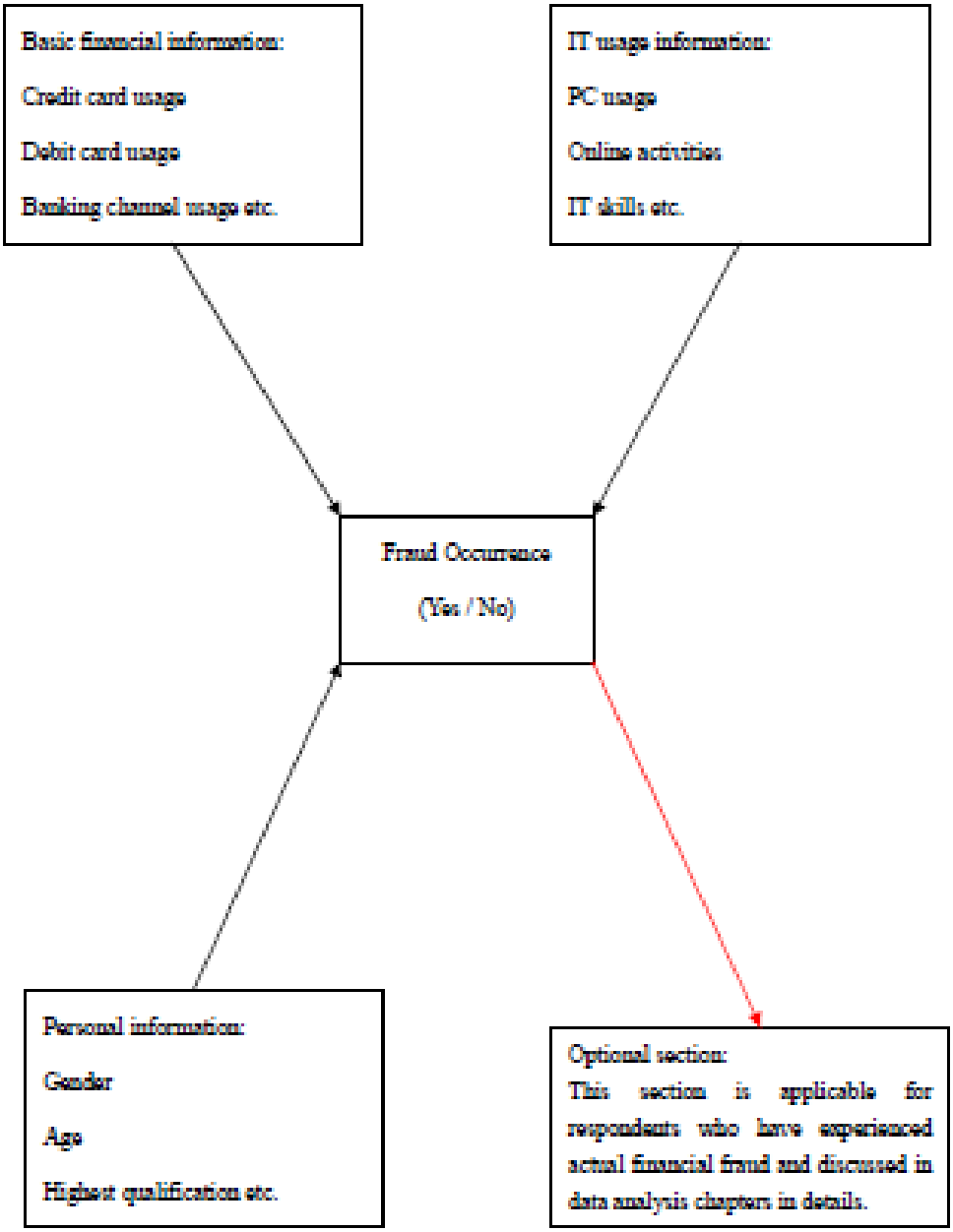


Figure 5.1 The framework of the study

5.7.2 Research hypothesis

Potential hypotheses are categorised into different groups based on the structure of the questionnaire. The individual hypotheses are based on reasonable prior belief, but there is no reason for them to be entirely consistent with each other – the data analysis will show which are supported and which are not. Prior work by Smith (2006) and Howcroft (2002) in related areas forms a basis for some of the hypotheses as indicated below.

(1) Hypotheses relating to Basic financial information. Similar hypotheses are to be found in Smith (2006) in his study of security issues associated with online banking.

- Customers who have more credit / debit cards are more likely to be defrauded;
- Customers who have longer history of usage of credit / debit cards are more likely to be defrauded.

The first hypothesis is self-evident between when comparing a response of zero and one, given that you cannot be defrauded if you do not have a card. However, those with a high number of cards could be more security conscious and so this effect could provide a counter leading to little significance overall. Similarly, the second hypothesis would appear to be self-evident but again there could be confounding effects.

(2) IT usage information

- Younger individuals are more confident with their IT skills;
- Individuals with higher qualifications are more confident with their IT skills (similar to Smith 2006);
- Customers who are more confident on their IT skills are more likely to be defrauded;
- Customers who use certain online activities are more likely to be defrauded;

Age and qualifications are standard items of demographic information used in these studies (eg in both Smith 2006 and Howcroft 2002). The third hypothesis in this group could go either way, depending on whether confidence is derived from ignorance or real appreciation of the dangers.

(3) Personal information

- Female customers are more likely to be defrauded than male customers;
- Aged customers are at less risk of financial fraud;
- Customers with higher qualification are less likely to be defrauded;

Demographic characteristics including gender, age, annual income, level of education and ownership of financial products are investigated in Howcroft et al (2002) in their investigation of the adoption of home based banking in the UK.

(4) Section dealing with actual cases of fraud
This section contains a further analysis of fraudulent cases to obtain more information about how and why these occurred and what action was taken by the various parties involved.

It is this latter area that is of particular interest. A major gap in the literature is individuals' attitudes to fraud and investigation of the factors which might make them vulnerable to fraud. Individuals who have experienced real fraud have had little attention in the literature and have not been studied in detail. One of the main purposes of this dissertation is to help to fill this gap which is why surveys in the UK and China were undertaken for this purpose.

5.8. Questionnaire design

5.8.1 Overview

Questionnaires in the literature, such as Howcroft (2002), Smith (2006) and Muthitacharoen (2006), group their questionnaires into sections, with the first containing a fair amount of demographic information so that the responses can be analysed in relation to such factors as age, education etc. A similar approach has been adopted in this thesis. The discussion of the previous chapters has raised a number of issues in relation to factors influencing electronic financial transactions and also the relative security of debit and credit cards. Of particular interest is any information that can be obtained about those individuals who have suffered actual financial fraud.

With this in mind, the questionnaire has been divided into four sections: (1) basic financial information; (2) IT usage information; (3) personal information; (4) a specific section for respondents who have experienced actual financial fraud. For the former three sections (1), (2) and (3), we focus on the individuals' basic information such as personal financial behaviours, IT skills and personal backgrounds. Those three sections are applicable for every respondent / household. The last part of the questionnaire, section (4) is designed for respondents who have suffered from actual financial fraud. In brief, section (4) asks for the information of any particular fraud cases.

Both in the covering letter of the questionnaire and the end of the section (3), we give clear instructions for this questionnaire and highlight the guides for the section (4) in particular. We expect to get replies from both respondents who have experienced financial fraud and who have not. The section (4) aims to collect detailed information about actual fraudulent cases. It starts from the fact / description of the fraudulent case by asking the money loss involved in; where / when / how the fraud occurred; following questions on payment methods / schemes used. Finally it deals with the customers' perception / satisfaction / awareness.

Both open and closed end questions are used in the questionnaire. For many questions with multiple options, extra space is reserved for respondents to write down their own statements. In particular, we put an optional question at the end of section (3) asking whether respondents would like to be contacted at their convenience, such as by phone, by post, by email or in person. The purpose is to invite respondents who are really interested in this study and willing to share specific information for future research.

5.8.2 Discussion of questions

As discussed in the last section, questions we are interested in are helping to profile individuals' financial behaviours and gather information about fraudulent cases. The starting point for the design of the questionnaire was the research done by Grazioli and Jarvenpaa (2000 July), who discussed deception and trust between online shoppers and merchants by examining consumers' evaluation of a real commercial

website and a fraudulent one. However, it only covered a certain type of online fraud: malicious webpage / internet hijacking. Also, Smith, A.D. (2006) discussed the security and comfort issues of online banking and A. Muthitacharoen *et al* (2006/7) addressed on online customers and sales channels strategies. However this questionnaire we designed extends previous studies in several important dimensions to make further contributions in the following aspects:

(1) Coverage of questions

24 ungrouped questions were used in the research of Smith, A.D. (2006) while 16 questions grouped into 5 sections were in the research of A. Muthitacharoen *et al* ((2006/7). For our study, 44 questions were asked and grouped into 4 sections: 17 questions are about personal financial behaviours, 6 are used to investigate IT usage, 7 are about personal information and 14 are used to gather information on actual financial fraud cases. The questionnaire has a wider coverage and clearer presentation than others.

(2) Completion of options

When question is asked for age, only four options were provided by Smith, A.D. (2006): 18-24, 25-36, 37-48 and 49+. The intervals between these four categories are different to each other which might cause problems to data analysis. Especially for the age group 49+ that makes information overloaded. Age group 49+ included too many age levels and missed valuable information. For example, 50-year and 70-year usually have different financial behaviours because of the big gap between two generations including social environment, education level, IT skills, banking system and life styles. The Age question we are using provided 7 options with the same interval for respondents: <=20, 21-30, 31-40, 41-50, 51-60, 61-70, >71.

Also, question 4 addressed by Smith, A.D. (2006) focused on the highest level of education provided options as following: High School, Some College, Bachelors degree, Master Degree and Higher Level. It was lack of precise definition for those different education levels, such as 'Some College', which would make respondents confused and put the individuals' trust at the risk.

Similar, Question 10 from Smith, A.D. (2006), when respondents were asked what they do when they access their accounts there were only 3 alternative answers provided: 1. pay bills, 2. check balances/ verify transactions and 3. all of the above. The option 2 was actually mixed two different activities: check balances and verify transactions. It would be helpful if these two were put into two separate answers instead of the one combination. Besides, still plenty of other reasons of accessing bank accounts were ignored. Differently, we use 10 different financial activities to describe personal finance appropriately: cash withdrawal, order cheque book, change PIN, money transfer, cash deposit, balance checking, change address, personal investment, regular payments (e.g. bills) and mortgage/ loan services.

(3) Design of questions

The way to ask and present questions is critical because mail / email survey doesn't involve any face to face interactions and direct explanations. It is suggested that questions and answers are made easy to understand and that research and professional terms are avoided. In the questionnaire of A. Muthitacharoen *et al* (2006/7), a 7-scale instrument was used to measure the preference level of product, transaction cost, social interaction, risk and attitude. Besides too many words being used to describe each scale, such as 1= brick and mortar store is much more favourable, 2= brick and mortar store is more favourable, 3= brick and mortal store is slightly more favourable, 4= neutral, 5= internet store is slightly more favourable, 6= internet store is more favourable and 7= internet store is much more favourable (Muthitacharoen *et al.* 2006/7).

11 out of 16 questions were presented using short professional terms without any further explanations like product availability, product variety, overall social experience etc. instead of completed questions in the questionnaire of A. Muthitacharoen *et al* (2006/7). For example, question 1: product availability, which would be much clearer and easier to be understood by respondents if it was a completed question like 'which store has a better product availability, internet store or brick and mortal store? Another example is question 4: product price, it could be converted into a question like 'considering the product price, do you prefer internet store or brick and mortar store?'

(4) Questions working in pairs

One of the consistency checks used in the questionnaire is the use of paired questions in which there is a logical relation between the pattern of the answers to two different questions. For example, in question 1.7: 'how many different personal banking channels have you been using?' respondents are requested to tick whatever options are appropriate: branch banking, postal banking, internet banking, telephone banking (staff involved) and auto telephone banking (e.g. action line).

The next question, 1.8 is: 'how long have you been using different banking channels?' The options of banking channels are the same as in question 1.7 but this time the question is asking for exact numbers in years. Then question 1.9 asks for the frequency of usage of different personal banking channels: 'how often do you use different banking channels per month?'. Consistency requires that it is the same banking channels that are filled in for each of these questions.

Clearly, question 1.7, 1.8 and 1.9 are relevant to each other focusing on individuals' usage of personal banking channels from particular aspects. If the respondent made a mistake by missing certain options in question 1.7, we can find out by checking answers to questions 1.8 and 1.9. For example, a respondent used branching banking and internet banking but missed to tick the option of internet banking in question 1.7. In question 1.8 we found that branch banking has been used for 10 years and internet banking for 3 years. Also in question 1.9, we found that the same respondent uses branch banking 4 times a month and internet banking 10 times a month. After checking all these three relevant questions, we are assured that this respondent did use internet banking but forgot to tick it in question 1.7. Questions working in pairs help guarantee the completion of the data. Otherwise, we have to use missing value to deal with similar situation which would cause information lost of data.

The potential disadvantages of questions working in pairs are that extra workload will be incurred in analysing the data, the length of the questionnaire will be increased and there might be unforeseen ambiguities that were not apparent at the design stage of the

questionnaire. In the latter case, inconsistencies in the responses should highlight any specific problems.

(1) Extra workload showed at the data coding and data entry steps. For instance, more than one question asking for individuals' usage of different banking channels, consequently, we need different codes / variables for each question. More questions also mean more data to be entered into SPSS date set for further statistical analysis.

(2) Increase the length of questionnaire. As discussed in section 5.9.2, a few tips about how to improve response rates to postal questionnaires. For example, a shorter questionnaire is generally getting better response rate then a longer one. Supported by the pre-test survey we conducted locally, the questions working in pairs did not cause confusions or difficulties to the respondents and response rate.

(5) Open ended questions

Different from A. Muthitacharoen *et al* (2006/7) and Smith, A. D. (2006), open ended questions were used in the questionnaire of our study to collect further information which may not be provided by fixed options. Particularly, in the section 4 which is exclusive to respondents who have experienced financial fraud. Blank space in this section provides options to respondents who like to describe fraudulent cases in their own ways. Also, for respondents who experienced financial fraud more than once, they need extra space to put details of each fraudulent case. In section 2, few open ended questions were used to describe online activities and IT training experiences because it is impossible to lay out all possible online activities and training programmes. On the other hand, too many options and words would make respondents confused and bored. We only listed the most popular options and leave a blank for respondents to fill in any others.

(6) Richness of information

The questionnaire was used for our study focusing the financial fraud in particular online financial transactions. With three compulsory sections 1, 2, 3 and an optional section 4, we can collect information from both individuals who have and have not experienced financial fraud using the same questionnaire. We run different tests to do

data analysis for reliable results based on the richness of the data and the variety of variables (dependent and independent).

(7) Anonymity of questionnaire

Different from surveys using a mailing list, our study is completely anonymous. All the questionnaires were sent out randomly without any mailing list with names and addresses. Also, we emphasized the anonymity of our study in the covering letter and assured respondents that they could not be traced. For our case, it is believed that anonymity helped to increase the response rate considerably.

With increasing awareness of identify fraud, a posted questionnaire with correct name and address or even an email address are very likely to make an individual worried and uncomfortable. Although, we leave some space for respondents to leave their contacts if they are happy to be contacted for further research, it's completely voluntary.

5.9. Sample selection / response rate

In this section, we discuss the sample selection and response rate in the UK. Due to a different social environment in China, we revise the data collection methods slightly and explain in detail in the chapter 8 data collection and analysis in China.

5.9.1 Sample selection

The location chosen for taking a survey sample is another important issue for data collection. The response rate of a mail survey in particular will depend on the demography of an area. We are not only interested in the number of the people who live in an area but also the characteristics of these residents in a certain area.

Loughborough, the biggest town in Leicestershire, as stated in Charnwood Community Profile (Charnwood Council 2005), 18.5% of the population are aged under 16 years while 17.4% are of pension age; there are 60,472 households in

Borough with an average household size of 2.42 persons; 82.8% of the working age population in Charnwood are economically active and the average household income in the Borough is £31.234.

According to the population estimated in 2004, the population of Loughborough is 57,560 (Charnwood Council 2005) plus over 12,000 students studying and living here at the university terms. Loughborough University can be dated to 1909 when a small technical institute was established by local county council. After decades of development and transformation, Loughborough University has been rewarded as the University of the Year 2008(Loughborough University). Generally speaking, younger consumers are more familiar with bank cards system because they are more interested in new IT products and more willing to involve in technique innovations than aged consumers.

The other reason that Loughborough was chosen is that the East Midlands has been the place with the highest increase of plastic card fraud between 2004 and 2007, according to the APACS (2008). According to the table below, plastic card fraud losses increased 52% in the East midlands in 2007, although as stated by APACS, the apparently big increase of fraud loss in East Midlands might due to the location of retailing head offices instead of exact location of fraud taking place, because the retailing head offices are in charge of communicating with APACS and reporting figures of fraud losses accordingly.

Table 5.3 Plastic card fraud losses on UK issued cards split by UK region 2004-2007
(All figures in **£** million)

Region	2004	2005	2006	2007	+/- change 2007
South East	**£**238.2	**£**207.3	**£**176.6	**£**178.7	+1%
North West	**£**40.2	**£**33.2	**£**35.7	**£**35.8	0%
West Midlands	**£**24.2	**£**20.3	**£**17.2	**£**24.4	+42%
Yorkshire and Humberside	**£**24.3	**£**27.3	**£**27.2	**£**24.1	-11%
East Midlands	***£30.8***	***£23.8***	***£15.0***	***£22.8***	***+52%***
South West	**£**12.7	**£**11.3	**£**9.7	**£**11.8	+22%
Scotland	**£**16.7	**£**13.9	**£**9.9	**£**11.5	+16%
North East	**£**8.1	**£**7.3	**£**6.8	**£**7.8	+15%
Wales	**£**7.3	**£**5.2	**£**5.7	**£**5.3	-7%
East Anglia	**£**8.7	**£**6.2	**£**5.4	**£**4.8	-11%
Northern Ireland	**£**1.1	**£**0.8	**£**0.7	**£**0.7	0%
UK total	**£**412.3	**£**356.6	**£**309.9	**£**327.6	+6%
Fraud Abroad	**£**92.5	**£**82.8	**£**117.1	**£**207.6	+77%
Total all UK cards	**£**504.8	**£**439.4	**£**427.0	**£**535.2	+25%

The sample used for this study consisted of local residents whose address had been chosen randomly. Several areas / streets in Loughborough were selected, covering areas with different family income levels; education / degree etc. In this study we are using street A, B, C and D standing for the real locations and post codes to preserve anonymity as promised in the covering letter. We considered each household as an individual case and sent out one copy of the questionnaire. The following table, compiled from Loughborough on-line data summarizes the characteristics of streets (Upmystreet) which were chosen for the survey:

Table 5.4 Background of various areas in Loughborough

Highlights	**Street A**	**Street B**	**Street C**	**Street D**
Family income	Very high	Medium	Medium	High
Interest in current affairs	Very high	Medium	High	High
Housing-with mortgage	Medium	High	Low	High
Education / degree	Very high	Medium	High	High
Couples with children	High	High	Low	High
Have satellite TV	Low	Medium	Low	Medium

The delivery time chosen was very early mornings over weekends in order to assure that questionnaires would stand a better chance to be noticed and filled during relaxing weekends.

5.9.2 Response rate

As we discussed in the section of data collection methods, one of the limitations of using a self-completion questionnaire, particularly by mail survey, is the lower response rate. A low response rate might result in the risk of bias on both data and findings. Bryman (2003, p136) mentioned that many published articles report very low response rate of studies compared to an ideal around 50 per cent suggested by some authorities. Because of low cost and easy administration, a mail questionnaire is still a very popular technique for data collection in social science. Bryman (2003) gave the following tips to improve response rates to postal questionnaires:

(1) Write a good covering letter. Several points have been addressed in my covering letter to introduce myself and my organisation; explain the importance of my study; guarantee the confidentiality of data.
(2) Enclose a stamped addressed envelope. We attached a printed freepost reply envelope with each questionnaire which can bring convenience to respondents and keep research cost low.
(3) Follow up and reminders. Generally speaking, follow-up or reminder is a very helpful solution to increase response rate, but it is not practical in this study because we are doing a completely anonymous survey to protect the respondents. We hoped also that this anonymity would increase the response rate.
(4) Shorter is better. As discussed in previous section, there is no clear definition for short or long questionnaire. To our understanding, if questionnaires target the suitable individuals and keep them interested in the topic, relatively long questionnaires will still work reasonably.
(5) Instructions and layout. We put an introduction to the questionnaire and clear instructions in the covering letter. For each question, we put a brief guide in small print after the question mark, such as, tick/ circle as appropriate. For the first two pages of the questionnaire, we left more space between questions to set up an easy start, leaving less space on subsequent pages at which point the individuals will have become more involved in the survey.

Apart from the steps we discussed above, there are two more aspects that need to be addressed to improve the response rate: firstly, the connection with local community, which is very helpful to increase response rate in my study. Having been a university town for decades, there has been a strong bond between university and local community in Loughborough in aspects of education experience, diverse careers and business opportunities. Residents are more familiar with university and more willing to become involved in an interesting research project.

Secondly, the research project should be interesting, advanced and practical. This project is about online financial transactions and financial fraud, which are raising more and more issues in modern daily life. Whether having experienced financial fraud or not, individuals are undoubtedly vulnerable to financial organizations,

merchants and criminals. In this case, individuals are keen to find out more about financial fraud in order to protect themselves.

5.10 Conclusion

In this chapter, we addressed the research methods used in this study. Also we explain the design of the survey questionnaire in detail based on the framework of my study. The sections about sample selection in China are in chapter 8 and the questionnaires in both English and Chinese can be found in the appendix. In the next chapter, the data analysis and SPSS results based on the data collected in the UK are analysed and discussed.

Chapter 6 UK Data Analysis and Summary

6.1 Introduction

In this chapter, we are focusing on the SPSS analysis results using data collected in the UK.

6.2 Data collection

6.2.1 Overview

A pre-test survey was carried out to a sample of 200 households in the Loughborough area. 59 replies were received and the responses were analysed carefully for signs of difficulty and ambiguity, and also to gauge where there might be some omissions. Following this exercise a few changes were made to the questionnaire in response to comments received. For example, question 1.13 was: 'Do you pay off your credit card every month? To the permitted responses of Yes and No was added 'Sometimes'. Three questions about passwords were also added and the covering letter was changed to explain more precisely the purpose of the study. Following this exercise the main survey was carried out. During two consecutive weekends, 1200 copies of survey were sent out randomly in residential area in Loughborough. In the following 6 weeks, 271 valid replies and 13 partially completed replies were received, giving a response rate of 22.6 %. All the replies were examined manually and data were entered into SPSS for analysis.

6.2.2 Data collection bias

Both in sampling and response, it is possible that data collection and analysis will be effected by bias leading to misleading results. Two potential biases that need to be considered are selection bias and response bias.

Selection bias occurs when sample is taken from a particular subset of the population with different characteristics to the population as a whole. To detect the selection bias, we can compare the summary statistics of the selected sample with those of the population as a whole (if known), or, if not known, take a sample from another part of the population and compare. The ideal solution to selection bias is to get more samples from different parts of the population.

Response bias refers to the tendency for there to be a higher response rates from individuals who have strong views, or have one particular view. To detect the response bias, we can compare the summary statistics from those who responded with the statistics from the population or with the statistics of those who did not respond. The ideal solution to the response bias is to increase the response rate, e.g. survey follow-up or reminder, which is not applicable in this study because of the required confidentiality and anonymity of the survey.

To test for selection bias we ideally need to know the characteristics of all individuals in the sample of 1,200. However, we only have the information from those who responded. A test on respondents only will conflate both selection bias and response bias, but nevertheless it is worth carrying out to test for bias generally. We could carry out the tests on any item of data for which there is population information, but we will illustrate with qualification data. For the respondents, 62.4% held a Bachelor degrees / Professional qualifications and further degrees. The national statistics show 41.5% of young people aged 18-30 going to university to study full time in 2003 (Walker, Zhu 2003). To test our sample against the national statistics we take as the null hypothesis H_0 that the population from which our sample is drawn has a mean of p=0.415, with an alternate hypothesis that it is higher. The standard error based on a binomial model with a sample size of 271 is calculated at 0.02993, the difference between 0.624 and 0.415 therefore representing 6.98 standard errors indicating that at all conventional levels of significance the population to which our respondents belong has a mean that is significantly higher than 0.415, or 41.5%. As the characteristics of the individuals in the full sample are not known, the extent to which this due to either selection or response bias cannot be answered. However, it is likely that selection bias is the major component.

Does this matter? It is contended that it does not, on the basis that we needed to carry out the survey in a location where the residents were more likely to have internet access because the study is about the financial transactions occurring on the internet. As suggested by Internet Access 2008, adults under 70 in the UK who had a degree equivalent qualification were most likely to have access to the internet in their home, at 93 per cent (UK National Statistics 2008). In short, people who have had better education are more likely to access to the internet at home. Considering the increase of educated population nationwide and proved connection between education and internet access at home, we would like to say that neither selection nor response bias is of any real consequence in this study.

6.3 Data Analysis-Summary (N=271)

In this section we select a key variable and then look at its relationship with other variables in the same grouping, these groupings being IT skills, age, gender, highest qualification, education background, usage of credit cards, usage of debit cards and usage of online activities. For example, in the section below, 'IT skills' is selected as the main variable. After looking at its distribution amongst the respondents, its relationship to age, then gender, being defrauded and highest qualification is investigated.

As an initial step, we show below descriptive statistics of two variables: age and gender.

Table 6.1 Age * gender Crosstabulation (UK)

			gender		
			male	female	Total
age	<20years	Count	1	1	2
		% within age	50.0%	50.0%	100.0%
		% within gender	.7%	.8%	.7%
		% of Total	.4%	.4%	.7%
	21-30years	Count	6	16	22
		% within age	27.3%	72.7%	100.0%
		% within gender	4.2%	12.5%	8.1%
		% of Total	2.2%	5.9%	8.1%
	31-40years	Count	9	23	32
		% within age	28.1%	71.9%	100.0%
		% within gender	6.3%	18.0%	11.8%
		% of Total	3.3%	8.5%	11.8%
	41-50years	Count	26	31	57
		% within age	45.6%	54.4%	100.0%
		% within gender	18.2%	24.2%	21.0%
		% of Total	9.6%	11.4%	21.0%
	51-60years	Count	24	24	48
		% within age	50.0%	50.0%	100.0%
		% within gender	16.8%	18.8%	17.7%
		% of Total	8.9%	8.9%	17.7%
	61-70years	Count	31	19	50
		% within age	62.0%	38.0%	100.0%
		% within gender	21.7%	14.8%	18.5%
		% of Total	11.4%	7.0%	18.5%
	>71years	Count	46	14	60
		% within age	76.7%	23.3%	100.0%
		% within gender	32.2%	10.9%	22.1%
		% of Total	17.0%	5.2%	22.1%
	Total	Count	143	128	271
		% within age	52.8%	47.2%	100.0%
		% within gender	100.0%	100.0%	100.0%
		% of Total	52.8%	47.2%	100.0%

(1) Scores of the general IT skills

The susceptibility to internet fraud might be expected to increase with the IT ability of the user at least up to the point where the user becomes more adept at applying protective measures. We provided seven options (from 1=very poor to 7=excellent) for the respondents to score their general IT skills. 78 out of 271 (28.8%) respondents scored their general IT skills 'average'. 20.7% and 19.6% respondents scored 'good' and 'very good'. 25.1% respondents admitted that the score of their IT skills was below the 'average' and ticked the categories labelled 'very poor', 'poor' and 'not good'.

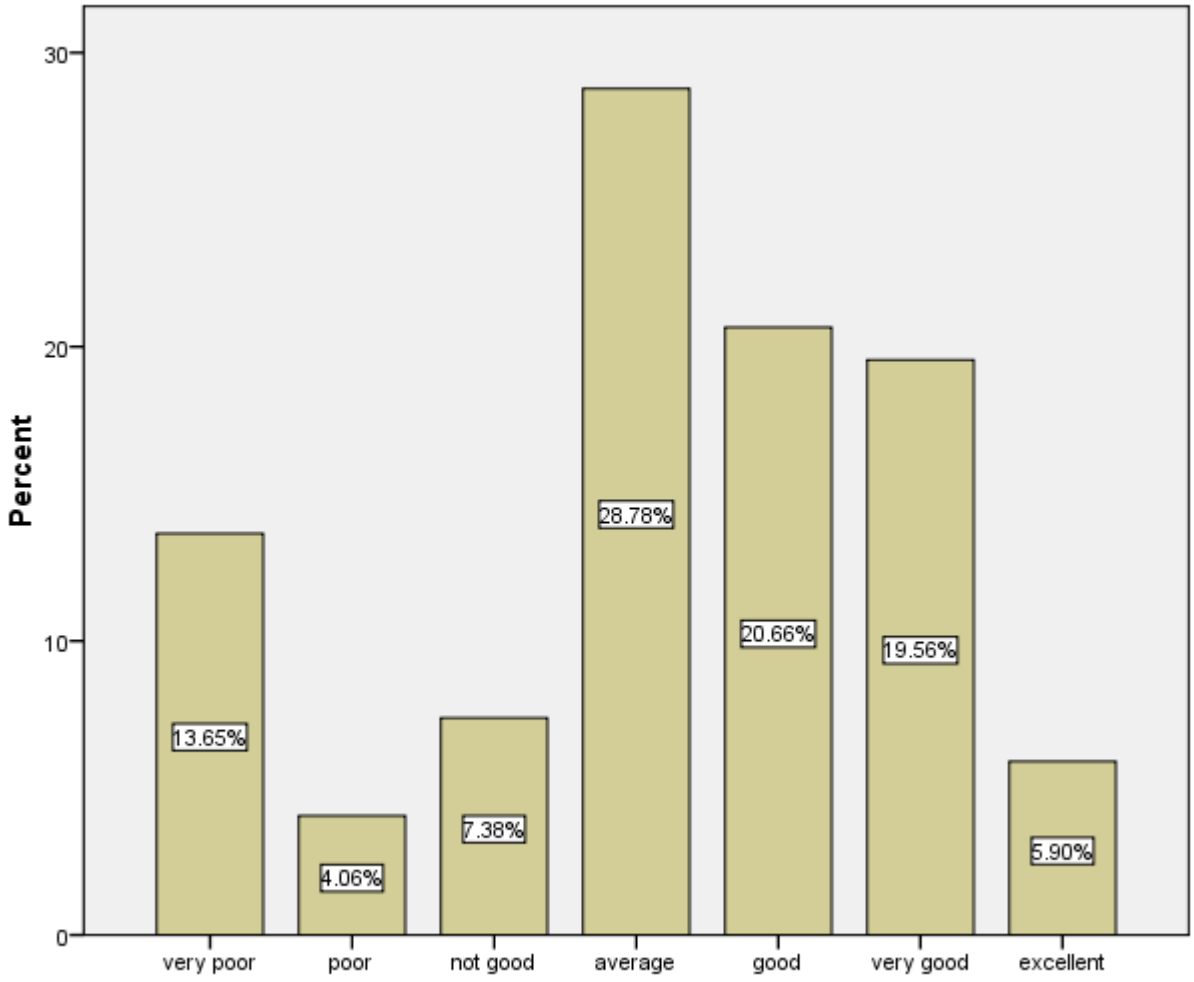


Figure 6.1 Overview of score of general IT skills

(1.1) General IT skills and different age groups

We split the variable 'general IT skills' into the different age groups, which have been categorised in the survey question as: <20 year; 21-30 years; 31-40 years; 41-50 years; 51-60 years; 61-70 years and >71 years.

Besides indication from the figure that aged respondents are less confident with their IT skills, a Chi-square test supported the hypothesis that older people are likely to see themselves as having lower IT skills, the correlation being negative (-0.601) and significant (0.000).

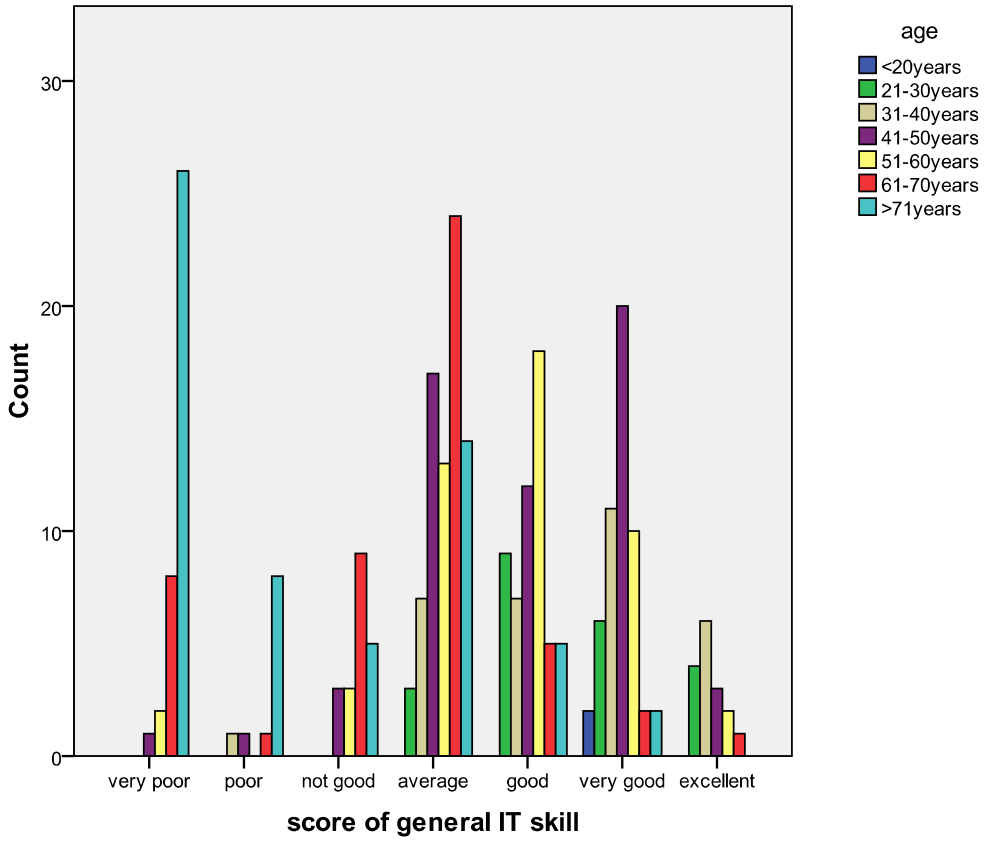


Figure 6.2 Age vs. self-assessed IT skills

(1.2) General IT skills and gender groups

As showed by the figure of the general IT skills score split by gender, we discovered that there is no big difference among the 6 out of 7 categories to describe 'the score of the general IT skills'. Only one category labeled 'very poor' IT skill showed any gender difference: male respondents who scored their IT skill as 'very poor' were twice as numerous as female.

As stated by the Internet Crime Report 2006, male customers are more likely to be victims of online fraud than female in the US[3]. However, based on our survey data, we found that there is no significant gender difference in relation to self-assessed general IT skills at the 5% significance level.

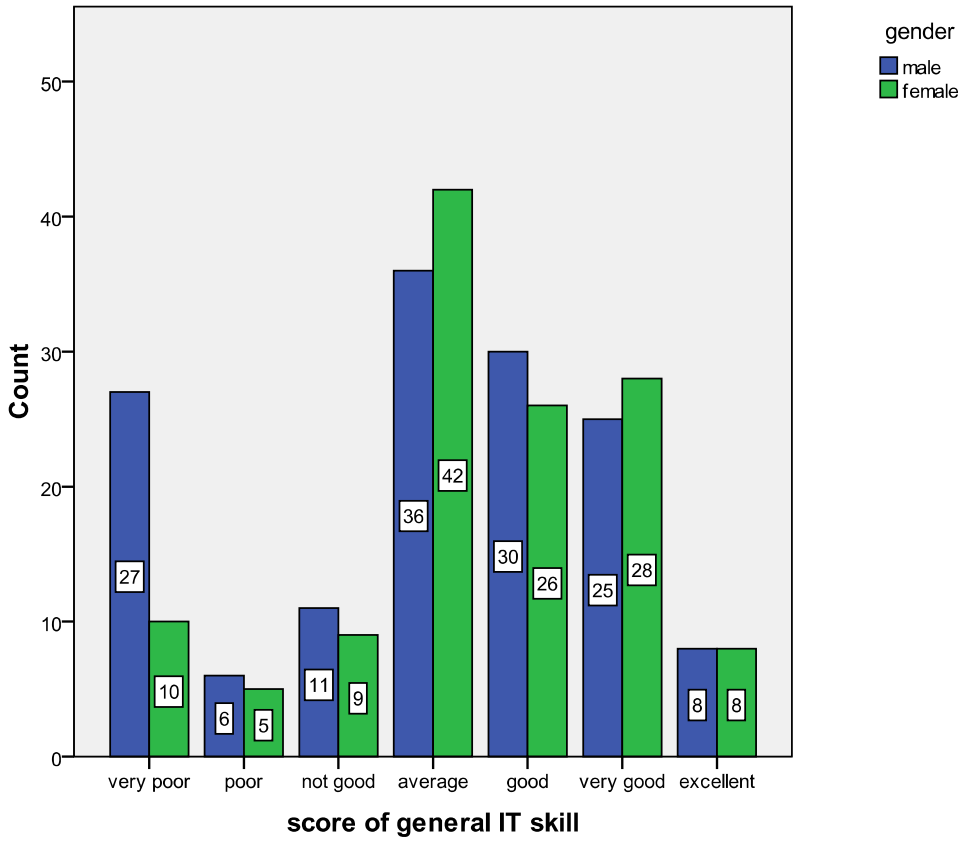


Figure 6.3 Gender vs. self-assessed IT skills

(1.3) Score of the general IT skill and fraud occurrence

Most instances of fraud were experienced by the respondents who were confident with their general IT skills. The most prominent green bars in the graph below were in the categories describing the individual's general IT skills as 'average', 'good' and 'very good'.

[3] Internet Crime Report 2006, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf (accessed 29-03-2010)

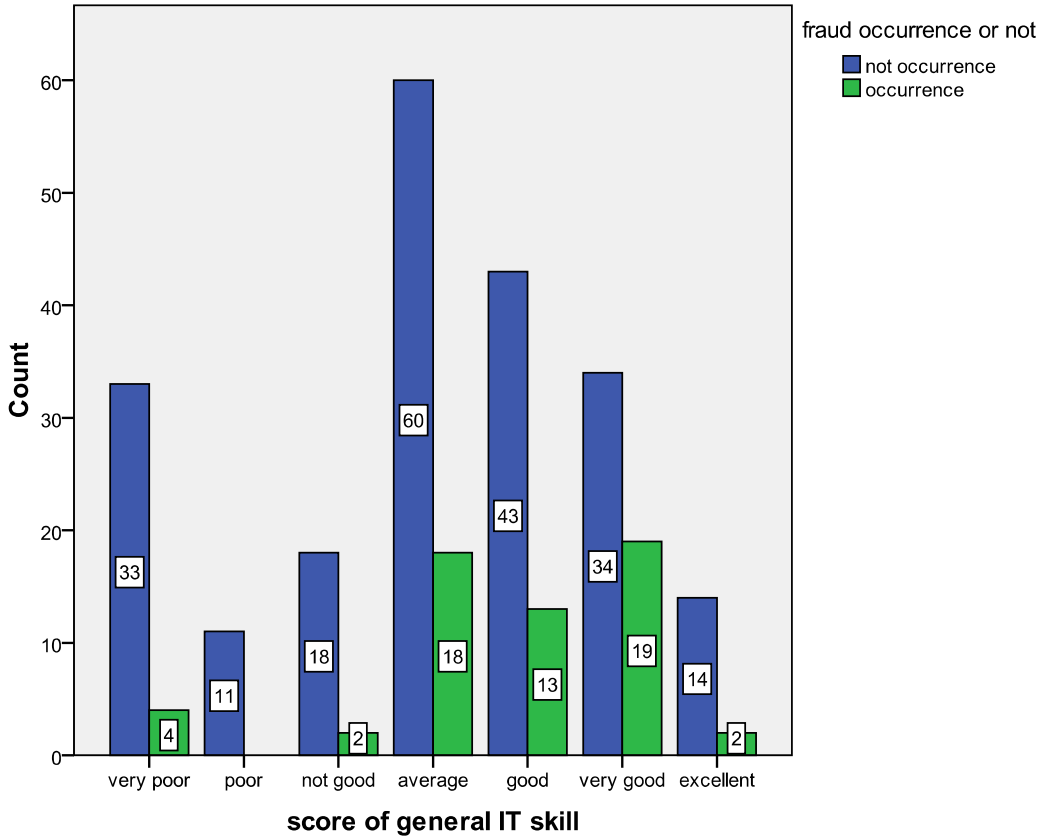


Figure 6.4 Fraud occurrence or not vs. self-assessed IT skills

The Chi-square results were consistent with this, indicating a significant positive relationship (sig value=0.011/ correlation value= 0.168) exists between general IT skill and fraud occurrence. In brief, people who perceive themselves to have better general IT skills are more likely to be defrauded on the internet.

The positive relationship between the general IT skill and fraud occurrence can be viewed in a number of different ways. Firstly, the scores given by respondents were based on self-evaluation and the answer was mainly based on the confidence of the respondents. Inevitably, some respondents could over estimate their IT skills. A second possible explanation is that we can not blame IT technology or IT skills for all fraudulent cases. As we discussed the different fraud schemes in the chapter 2 and 4, many schemes are not dependent on technology failure but are due to individuals' carelessness, or malicious actions by others. For example, individuals don't report lost-and-stolen bank cards to their banks on time; banks' customers reply to phishing emails releasing their personal information and banking details; bank cards details are

recorded by malicious cashiers and sold to criminals in the black market. A third explanation is that individuals with good IT skills are more likely to engage in on-line activities, thereby exposing themselves more to possible fraudulent activity.

(1.4) Score of the general IT skill and the highest qualification

Not surprisingly, the score of the general IT skill is related to the highest qualification. When we look at the purple and yellow bars which stand for BSC/ BA and further degrees (e.g. MSc / PhD) in the graph below, the top three purple and yellow bars fell into the categories 'average', 'good' and 'very good'. It indicated that respondents who have higher qualifications are more confident with their general IT skills.

The Chi-square gave us the same evidence showing a significant positive relationship between the general IT skill and the highest qualification. The sig. value is 0.000 which is smaller than 0.05 and correlation value is 0.202 which is positive. In brief, the results said that people who have higher qualification are more confident with their general IT skills.

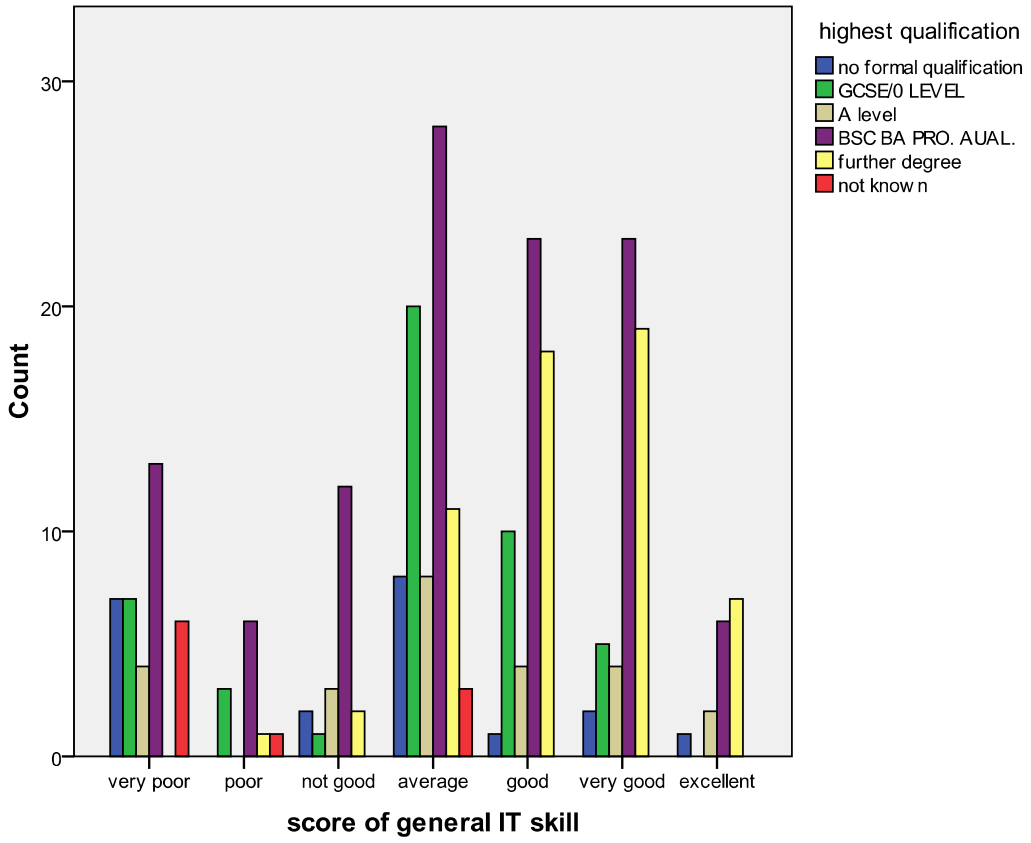


Figure 6.5 Highest qualification vs. self-assessed IT skills

(2) Age

Age is almost invariably included as an item of data in survey questionnaires directed at individuals. In deference to the sensitivity of personal information, particularly age related, we set seven ranges of age for respondents to tick. The figure below shows the age distribution of the respondents to the survey.

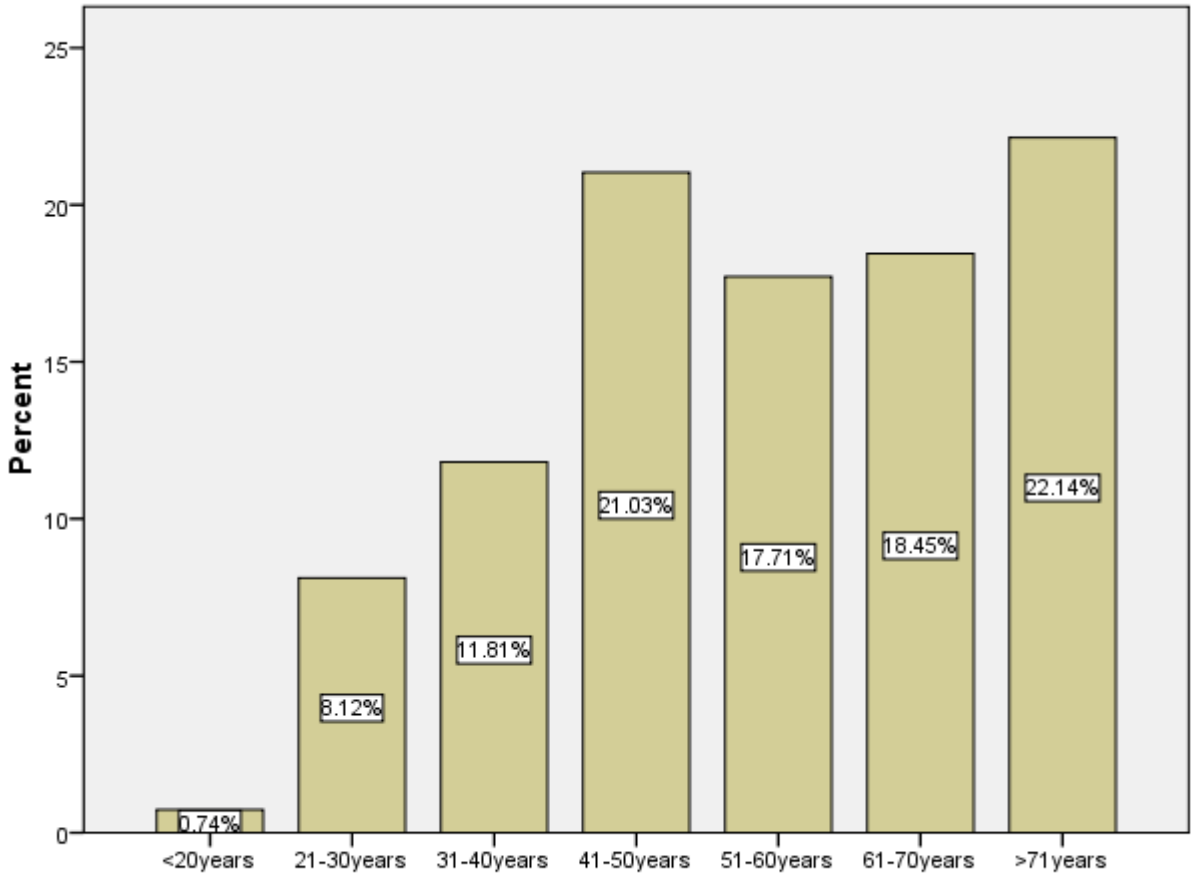


Figure 6.6 Overview of age

As can be seen from the graph, 60 out of 271 (22.1%) respondents were aged over 71 years. The respondents from this age group are perhaps more willing to participate because they have more spare time than others who more likely to work full time. However, their 'on-line' level of confidence and general experience of the internet is

limited so although they are keen to share their own experiences the amount of fraud they have experienced is limited, as is explored in the next section.

(2.1) Age and fraud occurrence or not

The figure below shows that fraud occurrence spreads across all the age groups, the green bars representing fraud occurrence. The age group 41-50 years is modal group – ie is most affected by online financial fraud, with fraud occurrence decreasing within groups which are older than 41-51 years while decreasing within groups as the age decreases below 41-51 years. The Chi-square test indicates a small but significant negative relationship (correlation value = -0.108, significance value 0.036) between Age and Fraud occurrence.

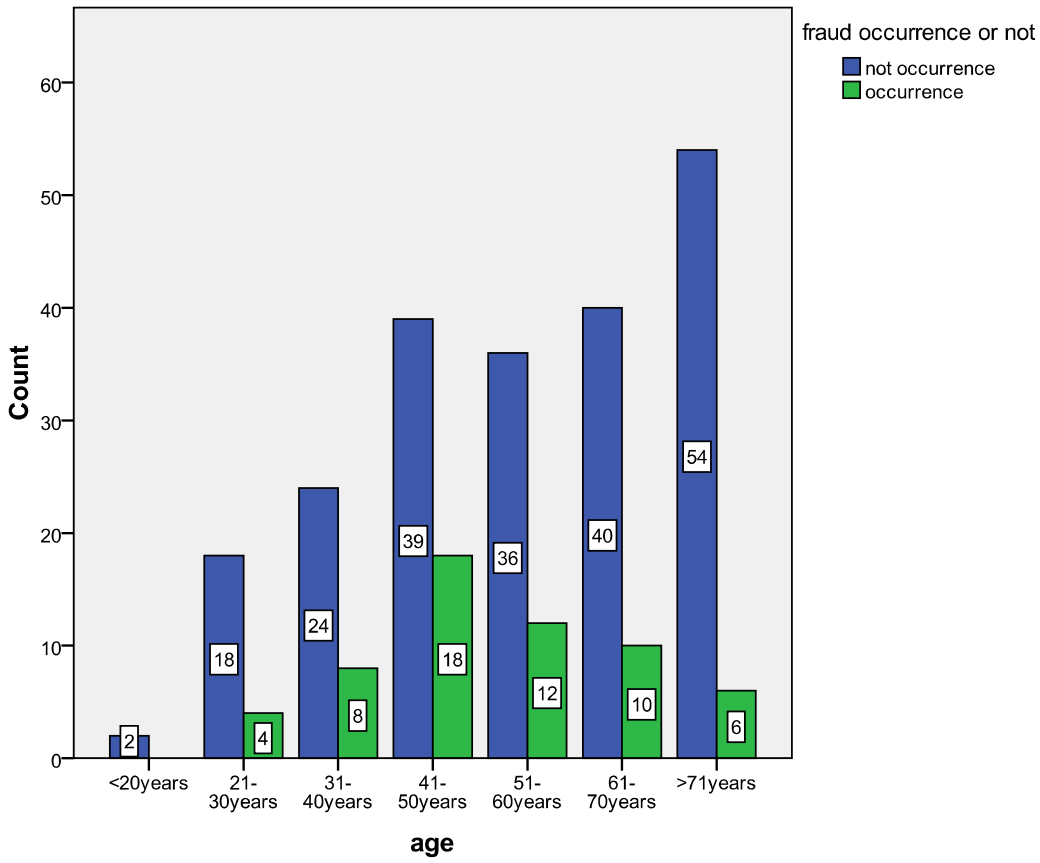


Figure 6.7 Age vs. fraud occurrence or not

However, to show the propensity to fraud within each age group we need to relate the incidence of fraud within each group to the number in each group. This is shown in the Table 6.2 below.

Table 6.2 Fraud Occurrence in relation to Age group

	AGE						
	<20	**21 - 30**	**31 - 40**	**41 - 50**	**51 - 60**	**61 - 70**	**>71**
Fraud occurrence	0	4	8	18	12	10	6
Number of respondents in group	2	22	32	57	48	50	60
% experiencing fraud	0	18.2	25.0	31.6	25.0	20.0	10.0

The table shows that the greatest propensity to experiencing fraud is in the 41-50 age group (31.6%) followed in equal measure by the 31-40 and 51-60 age groups, both at 25%. In order to discover whether there is any significant relationship between age and fraud occurrence, we look at the results from the Chi-square test (Chi-square value = 6.663; Sig. = 0.036; r = -0.108; Sig. = 0.076). Although there is a suggestion that younger respondents are more likely to be defrauded on the internet, the relationship is weak and not statistically significant.

Further, when we look at the correlation between age and different online activities, we found significantly negative associations appeared between age and each online activity: online shopping (r = -0.543; Sig. =0.000); internet banking (r = -0.416; Sig. = 0.000); online education service (r = -0.359; Sig. = 0.000); downloading media (r = -0.479; Sig. = 0.000). The correlation table suggests that older respondents are less likely to be involved in online activities. In particular, one third of the fraud occurred to the respondents aged 41-50, who probably have less spare time to familiarise themselves with using the latest internet technology.

(2.2) Age and Chip-and-PIN usage

The figure below showed that the group aged < 21 years only used the Chip-and-PIN scheme with debit cards (credit cards are not generally available to this group) and that some respondents in the group aged >71 years do not appear to use the Chip-and-PIN scheme with either credit cards or debit cards. It is possible that some members

of this group might find it difficult to adopt new technology, both in terms of remembering the PIN and also in terms of entering the PIN correctly using card readers.

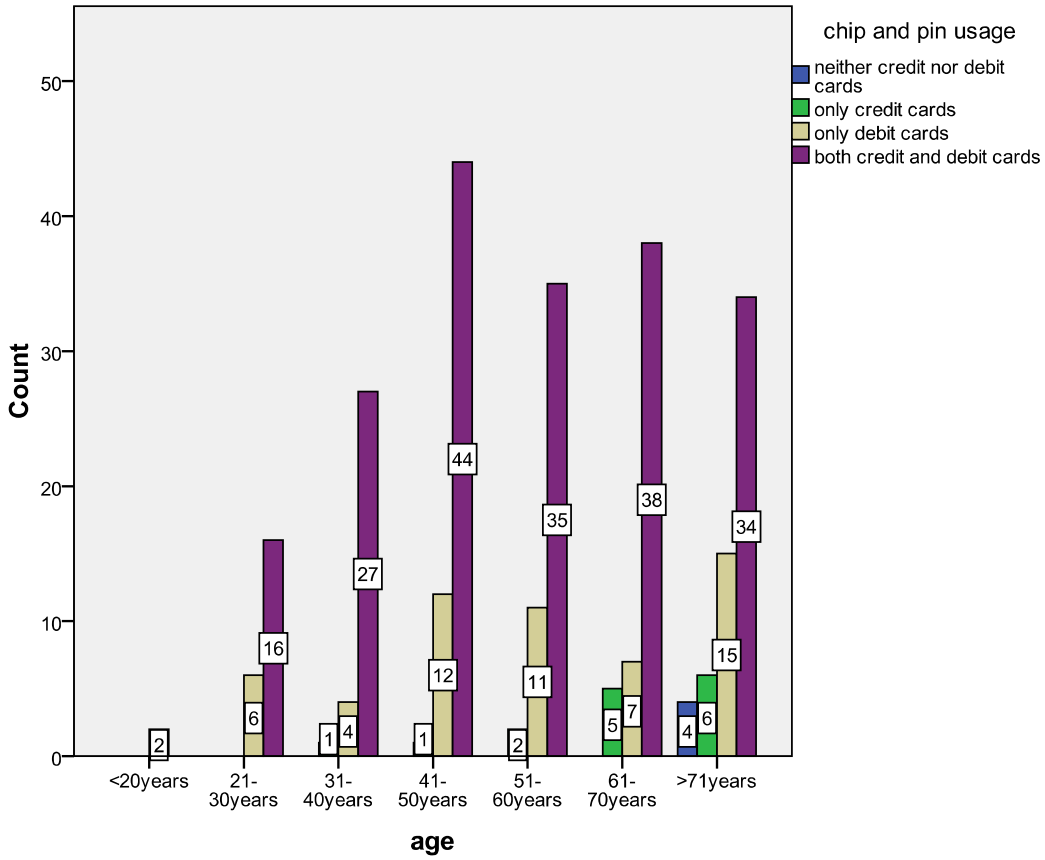


Figure 6.8 Age vs. Chip-and-PIN usage

As expected, most respondents had adopted Chip and PIN for both credit and debit cards. Where Chip and PIN was only adopted for either a debit card or a credit card, the number opting for a debit card was greater. This is as expected as a debit card is the normal means of withdrawing cash (as credit cards incur both a withdrawal fee and interest from the time of withdrawal), and in addition some people will always use a debit card in preference to a credit card.

(2.3) Age and pay off credit card monthly

The following figure shows evidence of a lifecycle effect, in that younger people have a lower propensity to pay off their credit cards every month whereas older people, who have more accumulated assets, tend to do so. However, there is an interesting

blip in that the 41-50 age group has more of a tendency to pay off their cards monthly than would be suggested by the trend in the data, suggesting perhaps that they are wealthier than expected on the basis of a simple trend.

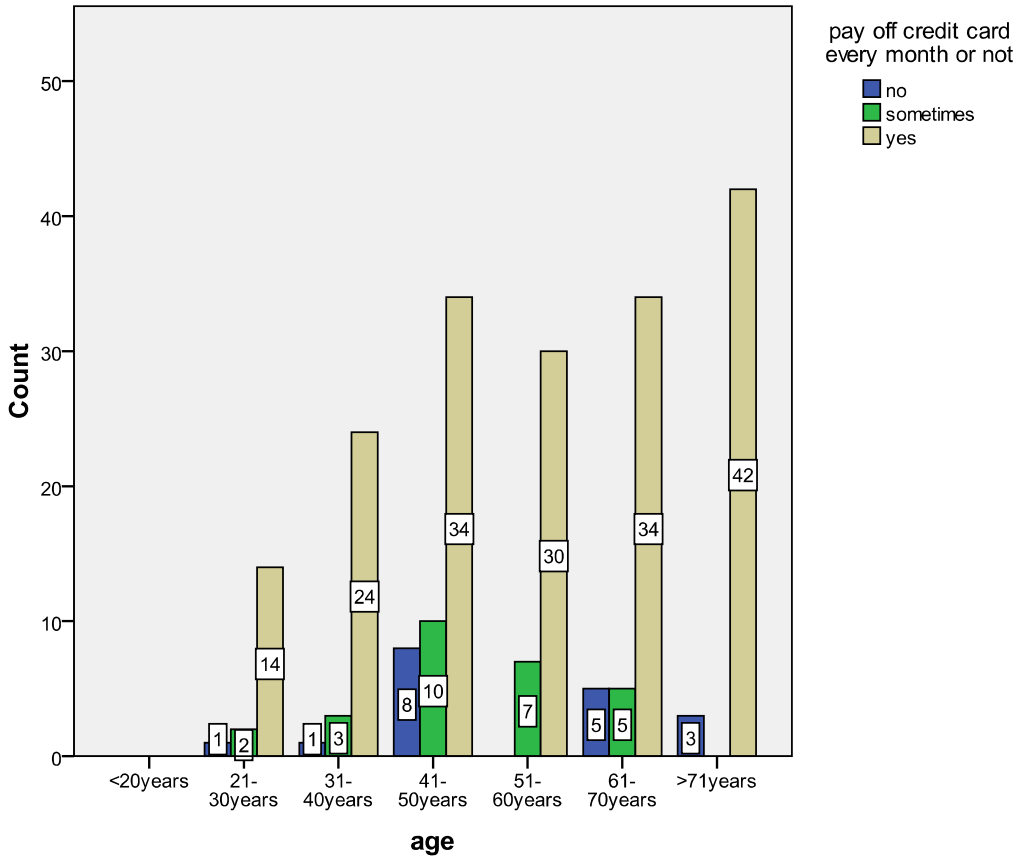


Figure 6.9 Age vs. pay off credit card every month or not

(3) Gender

The total number of valid responses in the survey conducted in the UK was 271. The number of male respondents was 143 (52.8%) and the number of female was 128 (47.2%). This difference is not significant at the 5% level (z = -0.92).

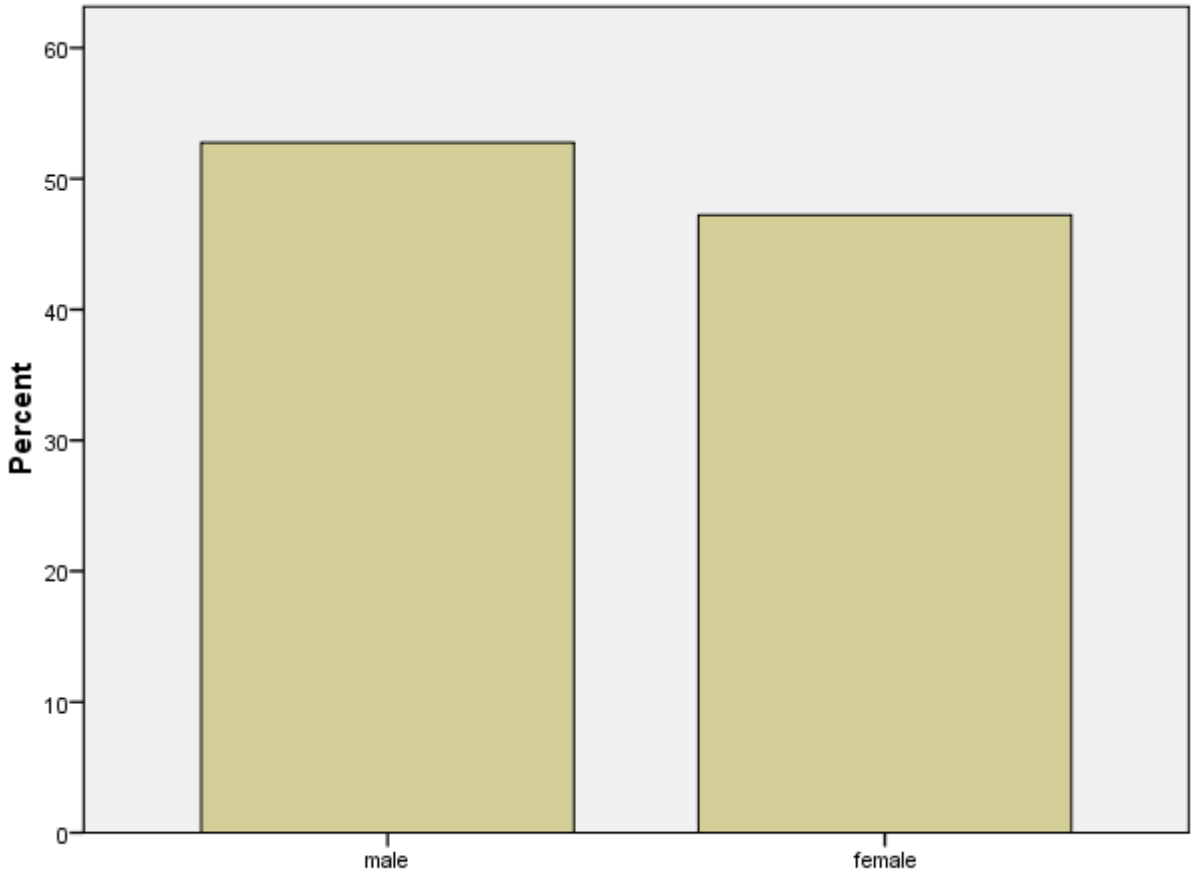


Figure 6.10 Overview of gender

(3.1) Gender and fraud occurrence

The figure below suggests that males are more susceptible to financial fraud than females, almost in the ratio 2:1 (ie 62.1% male to 37.9% female).

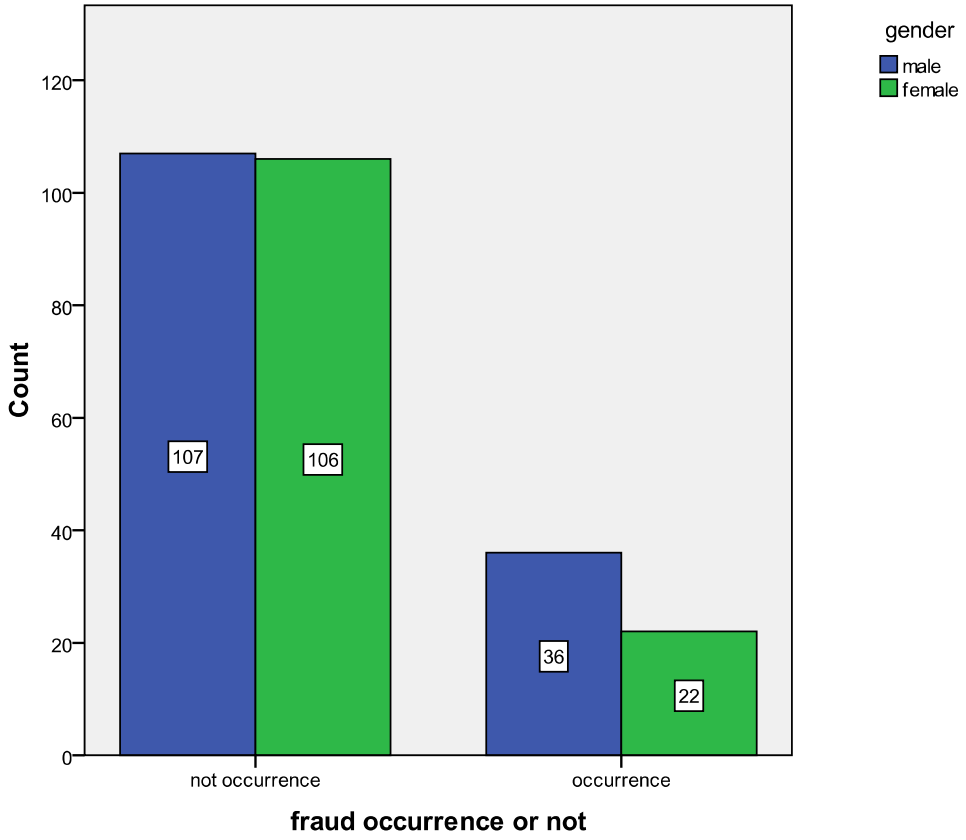


Figure 6.11 Gender vs. fraud occurrence or not

This is consistent with the Internet Crime Report 2006, which asserted that male customers were more likely to be victims of online fraud than female customers in the US[4]. In order to be able to assert this for the current study, a Chi-square test was carried out but interestingly the difference was not significant at the 5% level. This is because the proportion of individuals experiencing fraud is low, so if the overall mean results are applied to the numbers of males and females respectively, the expected number of males experiencing fraud would be 30.6 (actual 36) and females 27.4 (actual 22). The chi-squared statistic based on these small numbers turns out to be low and not significant (sig=0.109).

[4] Internet Crime Report 2006, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf (accessed 29-03-2010)

(4) Highest qualification

The respondents were asked to indicate which category described their highest qualification (if known). We gave six options for respondents to tick: No formal qualification; GCSE/ 0 LEVEL; A level; BSc/ BA/ Prof. Qual[5]; Further degrees and Not known.

The responses showed that 111 out of 271 (41%) respondents held a BSc/ BA/ Professional Qualification. 58 (21.4%) of respondents had further degrees, such as an MSc and/or a PhD. At the lower end, those for whom GCSE or 0-LEVEL constituted the highest qualification amounted to 46 (17%) and A-level holders 25 (9.2%).

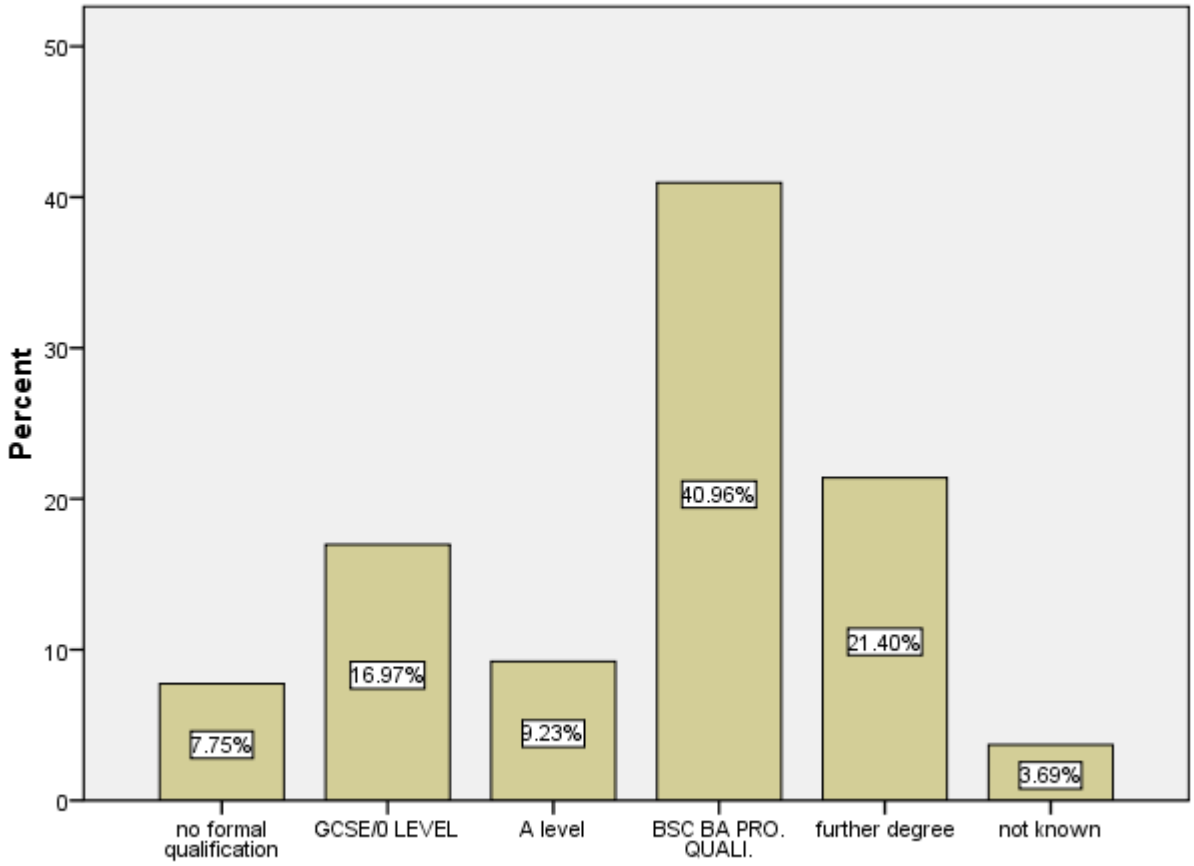


Figure 6.12 Overview of the qualifications of the respondents

[5] Professional qualifications include commercial pilots' licenses, police inspectors' examinations and attainments of similar standards as well as medical, legal and accountancy qualifications.

(4.1) Highest qualification and fraud occurrence

A Chi-square test was used to find out whether there was any significant relationship between the highest qualification and fraud occurrence, but no significant relationship was found. Although the highest number of incidences of fraud was in the BSc/BA/Prof Quali group, this was also the most numerous and the proportions are not significantly different.

The Chi-square test indicates a small but not significant relationship (correlation value = -0.103, significance value = 0.070) between highest qualification and Fraud occurrence.

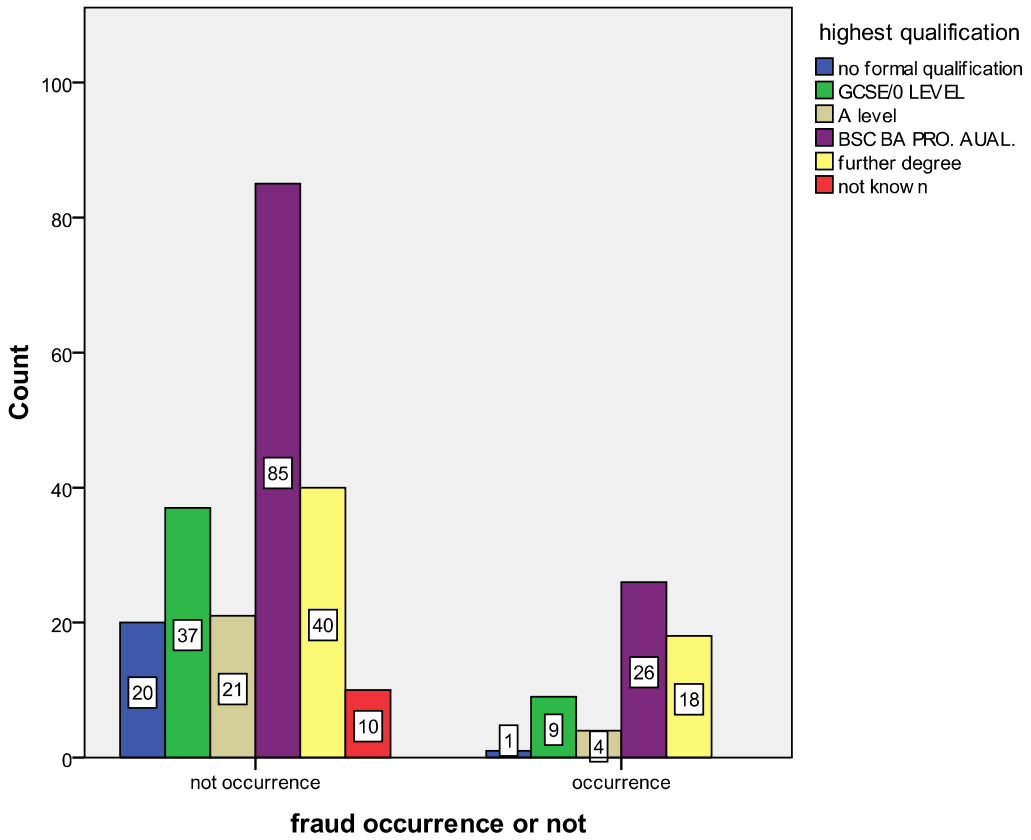


Figure 6.13 Highest qualification vs. fraud occurrence or not

However, to show the propensity to fraud within each qualification group we need to relate the incidence of fraud within each group to the number in each group. This is shown in the Table 6.3 below. We found that the most fraudulent cases appeared

within the group of respondents holding a further degree (e.g. MSc and PhD) at 31%. The second higher fraud rate appeared within the group holding BSC / BA/ Prof. Qualification at 23.4%.

Table 6.3 Qualification vs. fraud occurrence or not

Qualification	Fraud occurrence	Fraud not occurrence	Fraud rate (%)
No formal quali	1	20	4.8%
GCSE / 0 level	9	37	19.6%
A level	4	2	16.0%
BSC / BA/ Prof. Quali.	26	85	23.4%
Further degree	18	40	31.0%
Not known	0	10	0
Total	58	213	21.4%

(5) Education background: IT related or Finance related?

The purpose of this question was to investigate whether or not a background in IT or finance would make any difference to the incidence of internet fraud experienced.

From the 271 replies, 223 out of 271 (82.3%) respondents had studied neither IT nor Finance. 8.5% respondents (23 out of 271) studied Finance and 6.6% (18 out of 271) had studied IT. Only 7 out of 271 (2.6%) had an education background related to both IT and Finance.

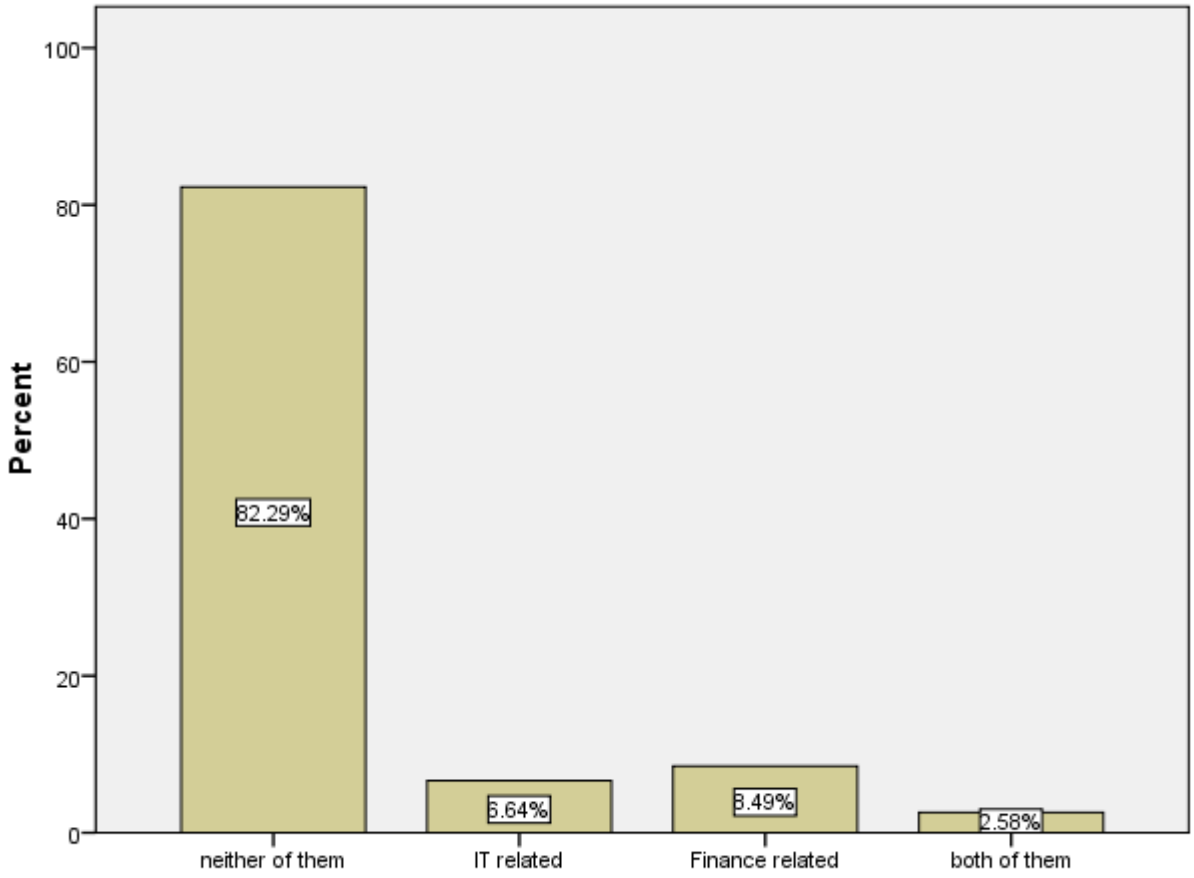


Figure 6.14 Overview of education background is IT related or finance related

(5.1) Education background is IT related / Finance related and fraud occurrence

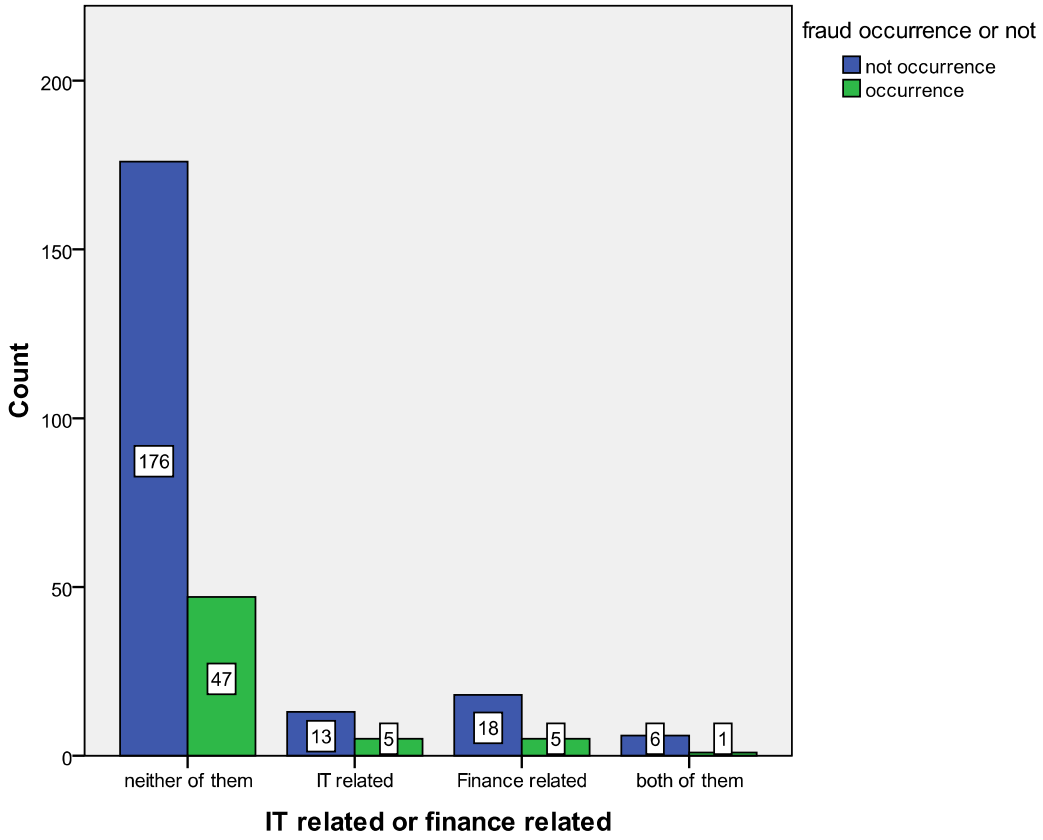


Figure 6.15 Education background vs. fraud occurrence or not

A Chi-square test to investigate whether a background in finance or IT impacted on the propensity to be defrauded suggested that there was no significant relation at the 5% level (correlation value = 0.012 and sig = 0.882).

Table 6.4 Fraud Occurrence in relation to education background

Education background (IT or Finance related)	Fraud occurrence	Fraud not occurrence	Fraud rate
Related to neither of them	47	176	21.1%
IT related	5	13	27.8%
Finance related	5	18	21.7%
Related to both of them	1	6	14.3%

(5.2) Education background is IT related / Finance related and age

Now we are investigating the education background split by age groups. As discussed in previous sections, seven age groups covered people aged <21 years to aged >71 years. The purple bar standing for age group 41-50 years is quite outstanding within the respondents whose education backgrounds are related to IT because respondents aged 41-50 years currently witnessed the development of IT technology from the very early stage and they were advantaged to be educated in IT technology.

Being one of the most popular subjects, Finance has longer history than IT technology in colleges and universities in modern society. For the respondents whose educated background related to Finance, we can see the red bar covering aged 61-70 years and blue bar covering aged >71 years are the first and second highest.

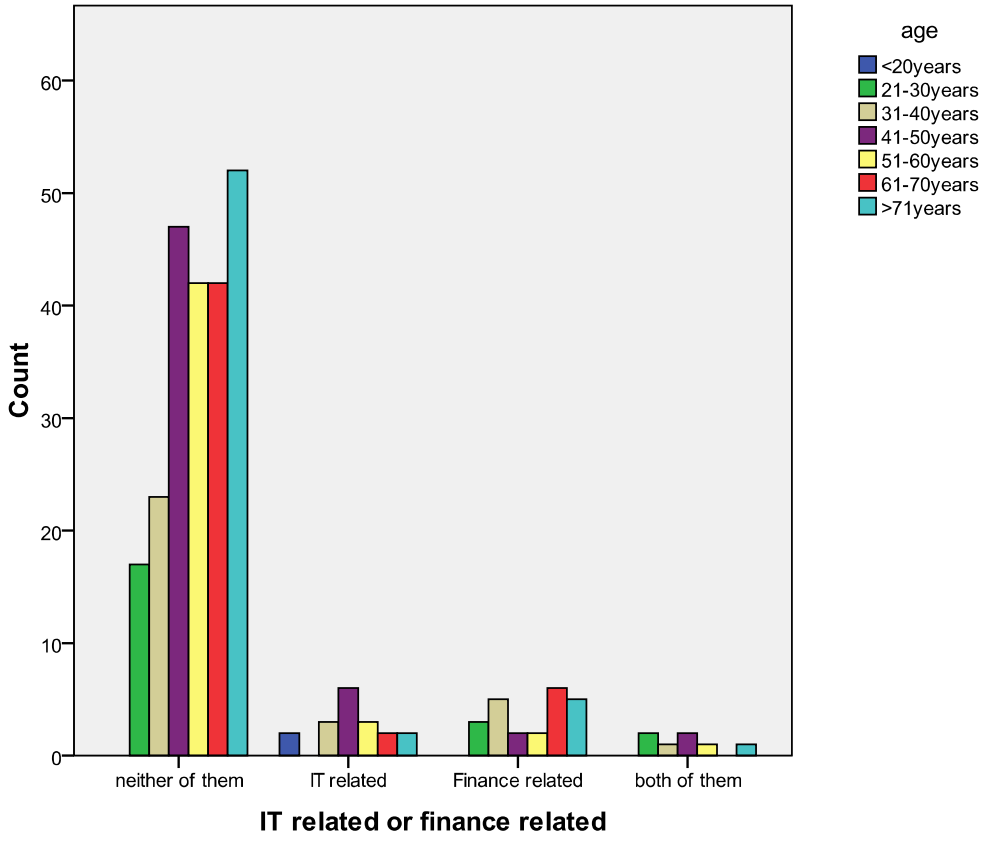


Figure 6.16 Education background vs. age

What is perhaps surprising is that there are a few respondents in the over 71 age group who have a background in IT. Within 60 respondents from the age group >71 years old, 52 held an education background related to either IT nor finance; 2 held a IT

related education background; 5 held a finance related education background and only 1 held an education background related to both IT and finance.

Table 6.5 Education background in relation to age

Age	Neither	IT related	Finance related	Both	Total
<20 Y	0	2	0	0	2
21-30 Y	17	0	3	2	22
31-40 Y	23	3	5	1	32
41-50 Y	47	6	2	2	57
51-60 Y	42	3	2	1	48
61-70 Y	42	2	6	0	50
>71 Y	**52**	**2**	**5**	**1**	**60**

(6) Usage of credit cards

(6.1) Number of credit cards

48 out of 271 (17.7%) respondents do not have any credit cards. At the other end of the scale, 2 out of 271 (.7%) respondents have 8 credit cards. In the current study the average number of credit cards held by respondents in the UK was 1.79. This compares with an average of 2.4 reported in a survey conducted in 2007 (gwade 17/03/2009).

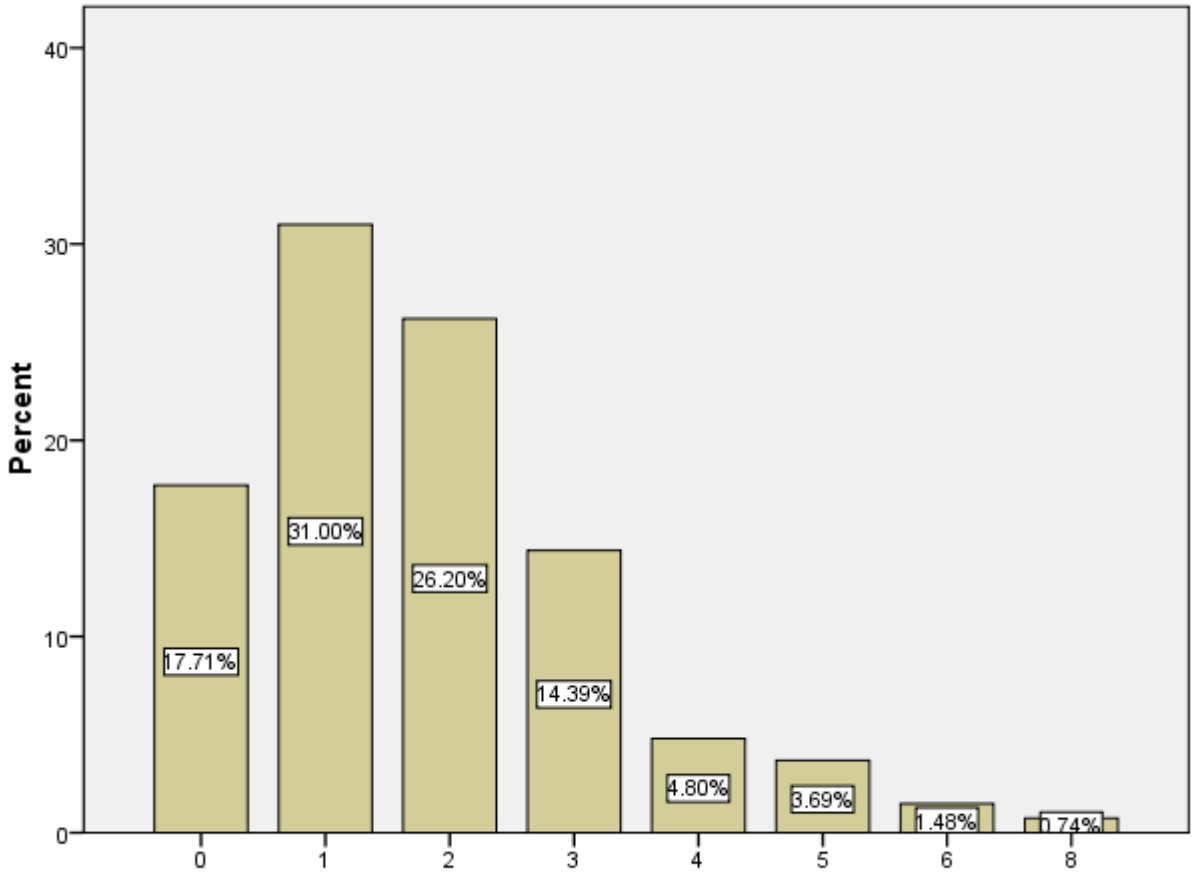


Figure 6.17 Overview of number of credit card owned

(6.2) Number of years of credit card usage

221 out of 271 replies provided answers giving the number of years of credit card usage, ranging from 1 year to 42 years. The average number of years of credit card usage in the sample is 19.36 years, this number reflecting the higher than expected number of respondents in the 71+ category (who may have held credit cards since their inception) and also the fact that at the other end of the distribution only 8.9% respondents are younger than 30 years old. The majority of the respondents (91.1%) fell into the age groups starting from 31 years, in particular aged from 41 to 70 years old. Note that round numbers predominate in the replies, indicating that the respondents found it difficult to give an exact number.

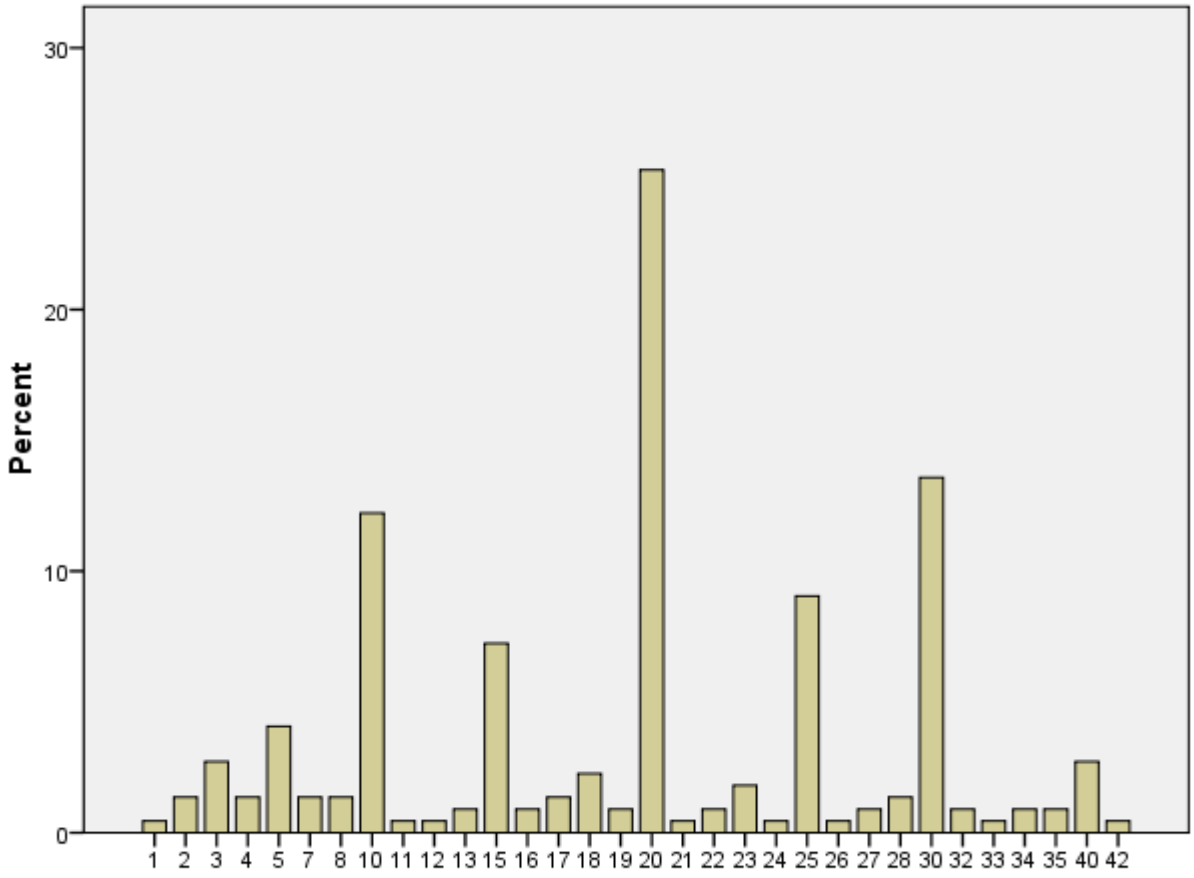


Figure 6.18 Overview of number of years of credit card usage

(6.3) Customers' satisfaction with credit card

We used five scales (from 1 to 5) to measure the customers' satisfaction with credit card services. 223 out of 271 respondents answered this question and the rest 48 respondents left the question blank. Those 223 valid responses fell into only four scales: not satisfied=2; average=3; satisfied=4 and very satisfied=5. None of the respondents click the 'not satisfied at all=1'. 217 of 271 respondents (80.1%) gave positive responses to the credit card services as follows: average 17.3%; satisfied, 37.3%; and very satisfied 25.5%.

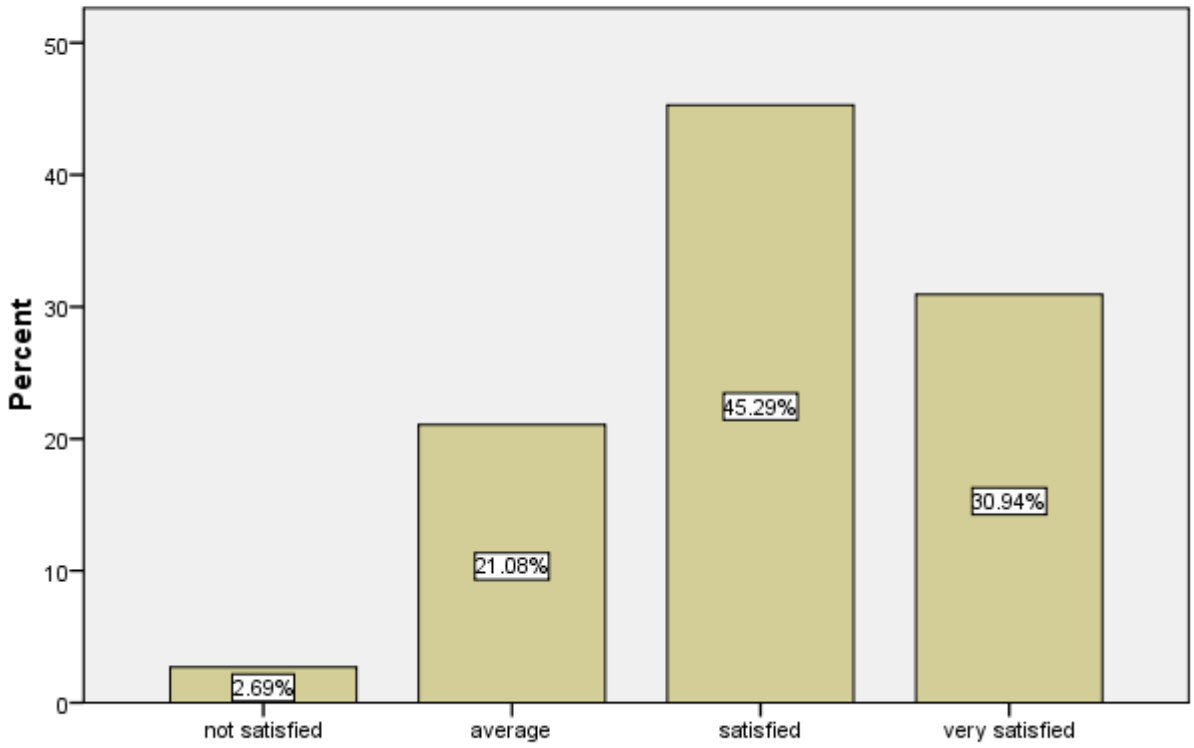


Figure 6.19 Overview of customers' satisfaction with credit card

(6.4) Customers' satisfaction with credit card and fraud occurrence

The green bars (on the right) representing fraud occurrence appear in each category for which there are responses, showing that except in a few cases the respondents were satisfied with the credit card services even when they had been subjected to fraud. Only 1 customer who had been defrauded gave a negative comment indicated a lack of satisfaction with the credit card services.

A Chi-square test to investigate whether customers' satisfaction with credit card impacted on the propensity to be defrauded suggested that there was no significant relation at the 5% level (correlation value = 0.034 and sig = 0.109).

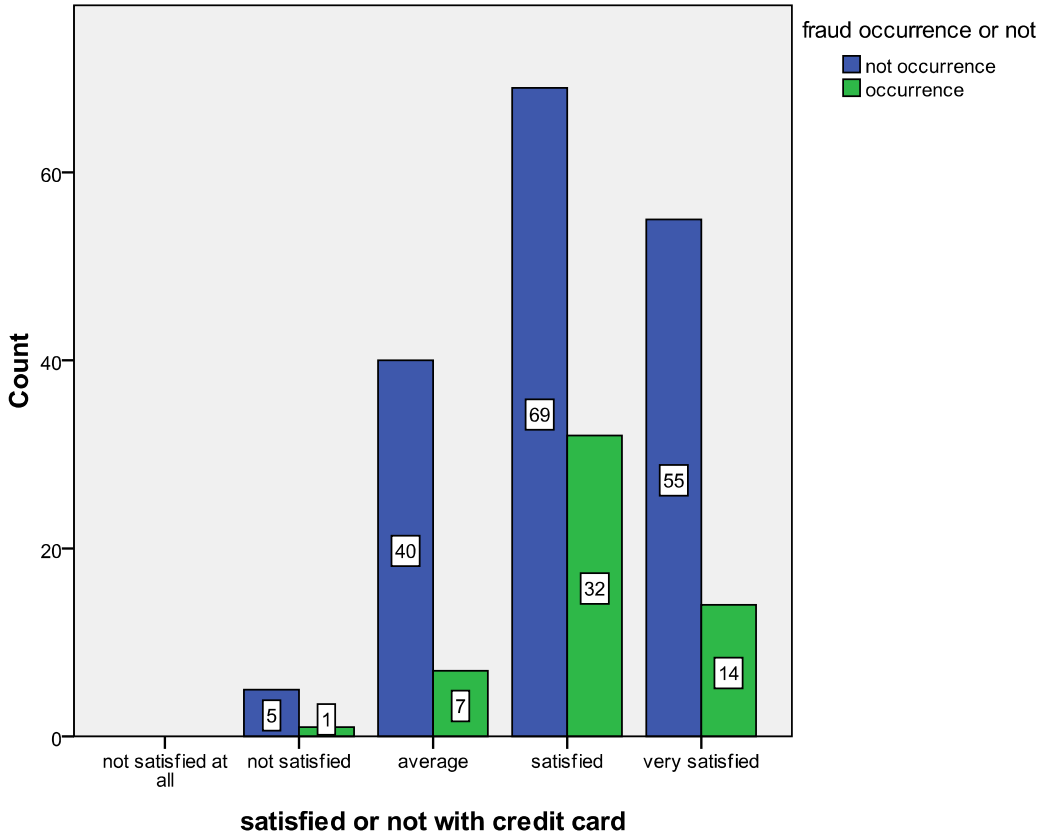


Figure 6.20 Customers' satisfaction with credit card vs. fraud occurrence

(7) Usage of debit cards

(7.1) Number of debit cards

The range of debit card holdings in the UK survey was 0 to 6, the average being 1.63. This is close to the figure of 1.6 in 2007 (gwade 17/03/2009). Only 5 out of the 271 respondents (1.8%) did not have any debit cards, for reasons discussed in section 6.1. However, the modal class was 1, consistent with the fact that most people only have one bank account.

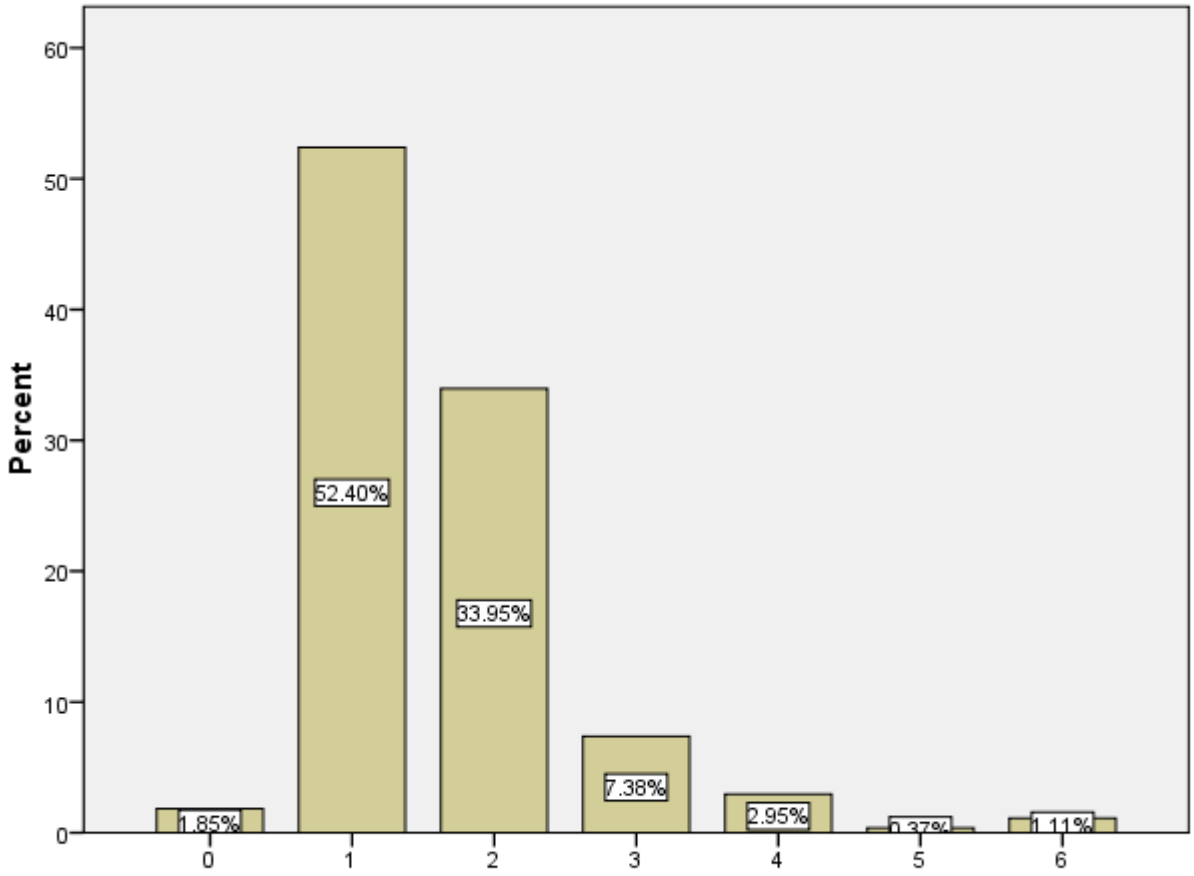


Figure 6.21 Overview of number of debit card owned

(7.2) History of debit card usage

264 out of 271 replies provided answers giving the number of years of debit card usage, ranging from 1 year to 40 years, the average being 18.1 years.

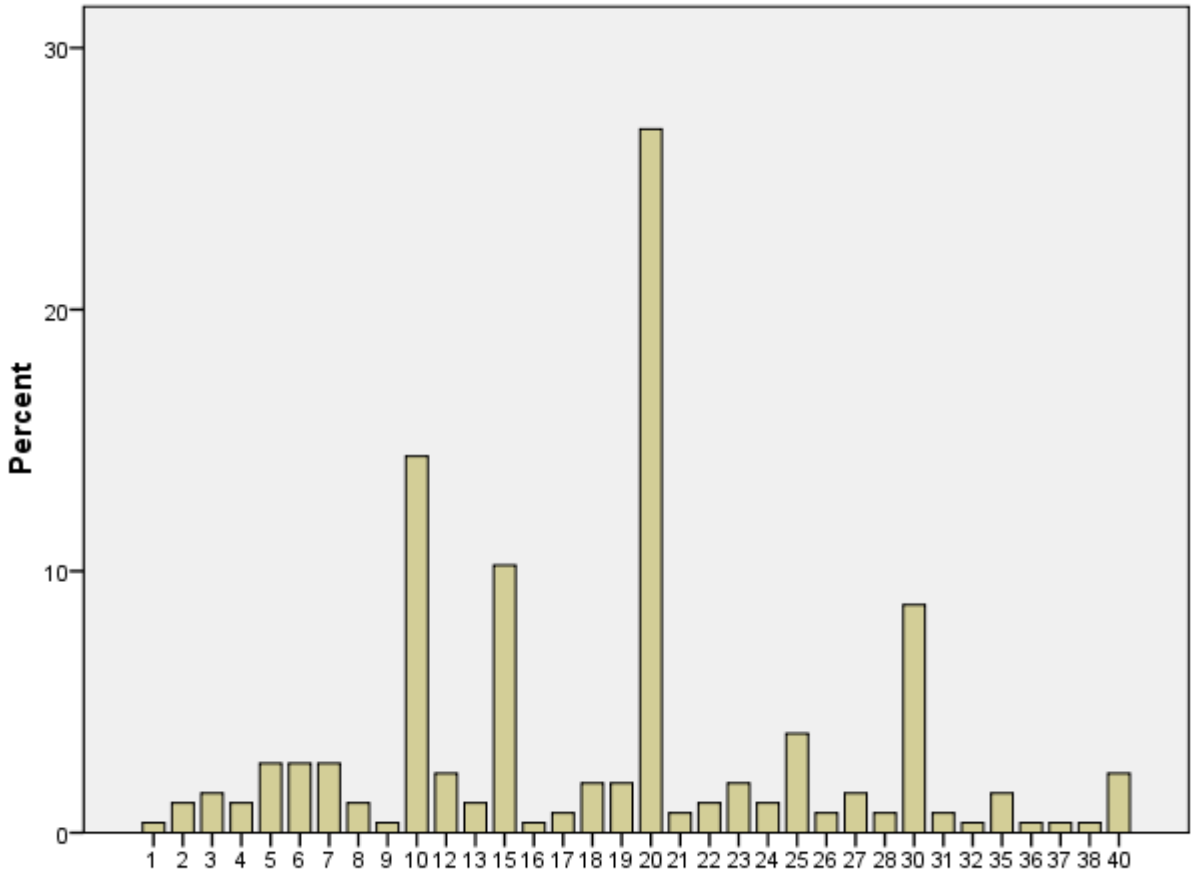


Figure 6.22 Overview of number of years of debit card usage

(7.3) Customers' satisfaction with debit cards

We used five scales (from 1 to 5) to measure the customers' satisfaction with debit card services. 266 out of 271 respondents answered this question and the remaining 5 respondents left the question blank. The 266 responses covered the full five scales: 1 = not satisfied at all; 2 = not satisfied; 3 = average; 4 = satisfied, and 5 = very satisfied. 261 out of 271 respondents (96.3%) gave positive responses to the debit card services, i.e. 9.6% average; 43.3% satisfied and 43.5% very satisfied.

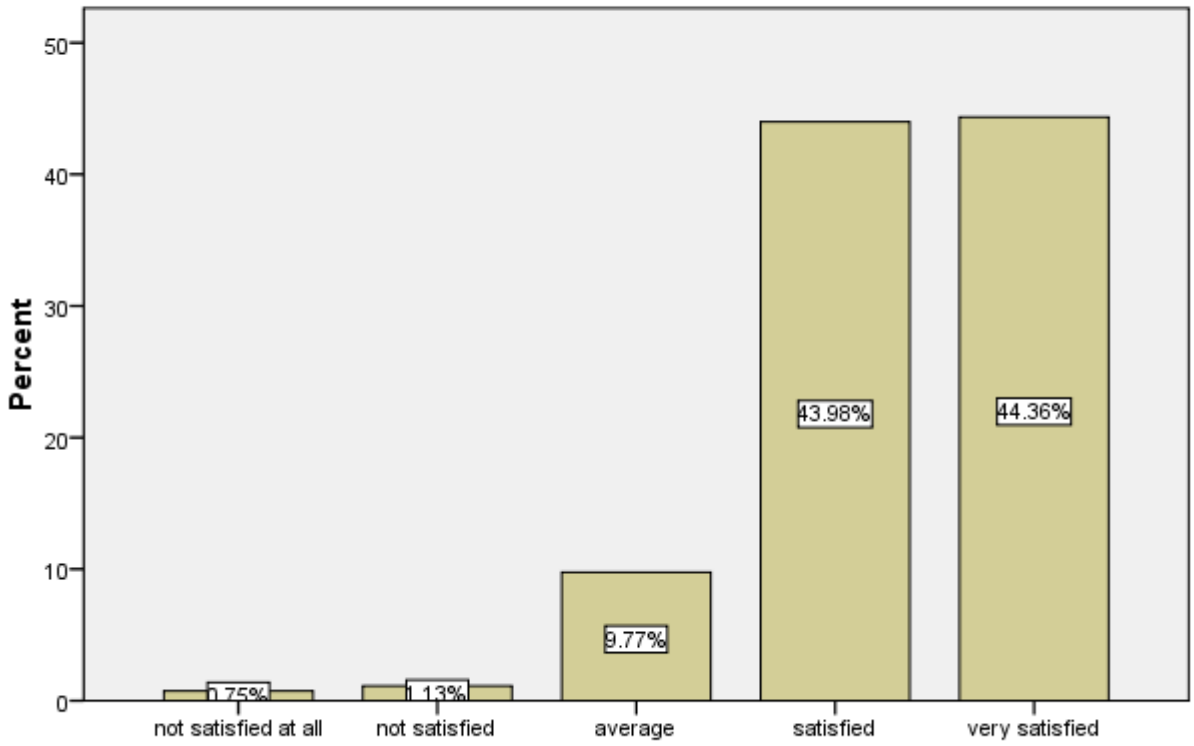


Figure 6.23 Customers' satisfaction with debit card usage

(7.4) Customers' satisfaction with debit cards and fraud occurrence

The green bars standing for fraud occurrence appear in three categories: average, satisfied and very satisfied, showing that most of the respondents who had been defrauded felt satisfied with the debit card services. It appears that defrauded customers are pleased with how the banks / credit card companies dealt with fraudulent cases, and suggests that there might be marketing value in further promotion of this aspect of the services provided.

A Chi-square test to investigate whether customers' satisfaction with debit cards impacted on the fraud occurrence suggested that there was no significant relation at the 5% level (correlation value = -0.063 and sig = 0.122).

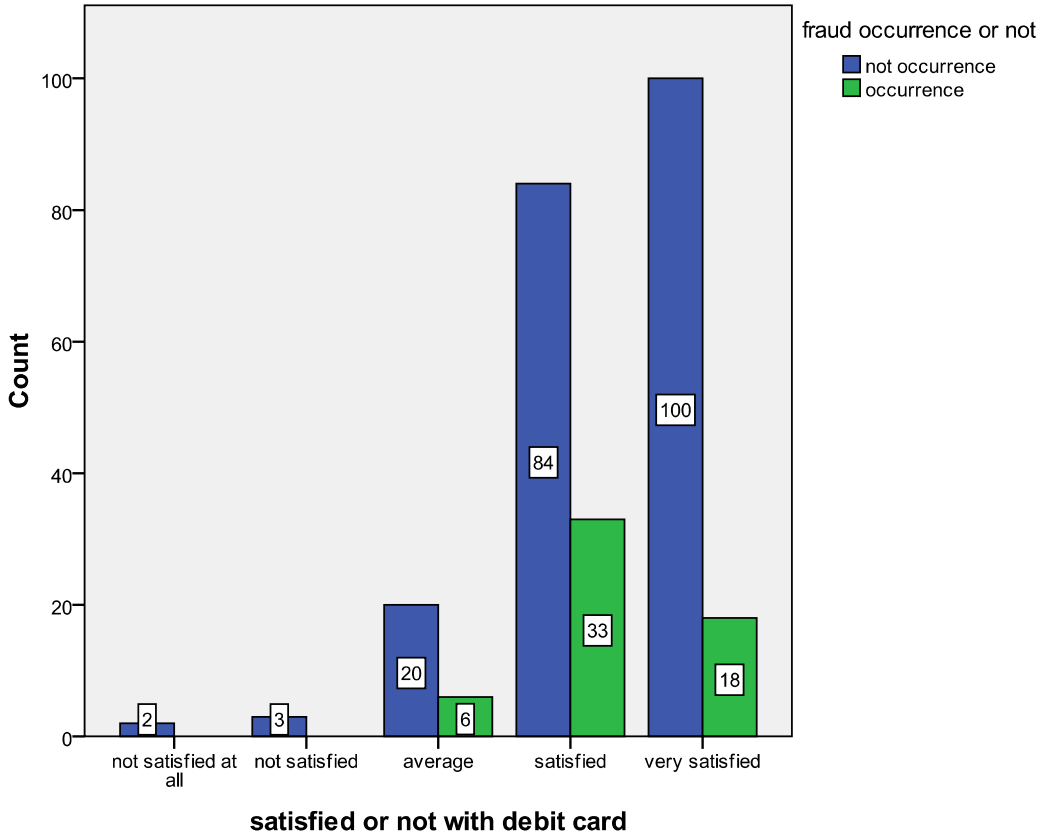


Figure 6.24 Customers' satisfaction with debit card vs. fraud occurrence

(8) Usage of online activities vs. fraud occurrence or not vs. age

In this section, the connection between experiencing fraud and use of a range of online activities is explored, the objective being to investigate if the use of such online activities leads to a higher propensity for the individual to be defrauded.

Table 6.6 Usage of online activities

Online activities	**Use of online activities**		**Correlation with fraud occurrence**	**Sig.**
	Yes	No		
Internet banking	155 (57.2%)	116 (42.8%)	0.215	0.000
Online shopping	182 (67.2%)	89 (32.8%)	0.212	0.000
Downloading media	77 (28.4%)	194 (71.6%)	0.210	0.001
Online education service	73 (26.9%)	198 (71.1%)	-0.053	0.381

(8.1) Usage of internet banking

116 (42.8%) of the 271 respondents were not using the internet banking while 155 (57.2%) were. In relating internet banking to being defrauded, a Chi-square test revealed a highly significant positive relationship between the usage of internet banking and fraud occurrence (correlation = 0.215, significance value = 0.000). This suggests strongly that internet banking users are at higher risk of internet fraud occurrence.

(8.2) Usage of online shopping

89 out of 271 (32.8%) respondents were not using online shopping compared to 182 (67.2%) who were. A Chi-square test indicated a highly significant positive relationship between the usage of online shopping and fraud occurrence (correlation value = 0.212, significance value = 0.000), implying that online shoppers are at higher risk of internet fraud occurrence.

(8.3) Usage of downloading media

194 (71.6%) out of 271 respondents were not downloading media from the internet and 77 (28.4%) respondents were. A significant positive relationship was found between the downloading of media and fraud occurrence (correlation value = 0.210, sig. value = 0.001), suggesting that downloading media users are at higher risk of internet fraud occurrence.

(8.4) Usage of online education service

198 (73.1%) out of 271 respondents were not using online education services and 73 (26.9%) respondents were. A Chi-squared test did not reveal a significant relationship between the usage of online education service and fraud occurrence, (correlation value = -0.053, sig. value =0.381) suggesting that online education service users are not at higher risk of internet fraud occurrence than non-users in the UK.

(8.5) Correlations between online activities vs. age

Considering the survey data we collected in the UK are mainly categorical, in particular the data used to describe variables like online activities and age; we

conducted Spearman's correlation coefficient, a non-parametric statistic to look for relationships[6].

Table 6.7 indicated that the correlations between selected online activities and age. The significantly negative associations appeared between age and each online activity: online shopping (r = -0.543; Sig. =0.000); internet banking (r = -0.416; Sig. = 0.000); online education service (r = -0.359; Sig. = 0.000); downloading media (r = -0.479; Sig. = 0.000). In summary, the correlation table suggested that younger respondents are more likely to involve in online activities. On other hand, older respondents are less likely to involve in online activities.

The correlations (Spearman Correlation＝r) between different online activities in Table 6.7, showed different strength of the association related to each other. Usage of online shopping is positively related to usage of internet banking (r = 0.586, sig.= 0.000); usage of online education services (r = 0.230, sig.=0.000) and usage of downloading media (r = 0.388, sig.= 0.000). Usage of internet banking is positively related to usage online education services (r = 0.189, sig.= 0.002) and usage of downloading of media (r = 0.330, sig.= 0.000). Usage of online education services is positively related to usage of downloading media (r = 0.337, sig.= 0.000).

[6] Andy Field, 2009, discovering statistics using SPSS, third edition, pp166-179.

Table 6.7 Spearman correlation table (online activities and age)

			usage of online shopping	usage of internet banking	usage of online education services	usage of downloading media	age
Spearman's rho	usage of online shopping	Correlation Coefficient	1.000	.586**	.230**	.388**	-.543**
		Sig. (1-tailed)	.	.000	.000	.000	.000
		N	271	271	271	271	271
	usage of internet banking	Correlation Coefficient	.586**	1.000	.189**	.330**	-.416**
		Sig. (1-tailed)	.000	.	.001	.000	.000
		N	271	271	271	271	271
	usage of online education services	Correlation Coefficient	.230**	.189**	1.000	.337**	-.359**
		Sig. (1-tailed)	.000	.001	.	.000	.000
		N	271	271	271	271	271
	usage of downloading media	Correlation Coefficient	.388**	.330**	.337**	1.000	-.479**
		Sig. (1-tailed)	.000	.000	.000	.	.000
		N	271	271	271	271	271
	age	Correlation Coefficient	-.543**	-.416**	-.359**	-.479**	1.000
		Sig. (1-tailed)	.000	.000	.000	.000	.
		N	271	271	271	271	271

**. Correlation is significant at the 0.01 level (1-tailed).

As stated by A. Field (2009): 'R^2 (coefficient of determination) is a measure of the amount of variability in one variable that is shared by the other'. If we look at the relationship between age and usage of online shopping, those two variables have a correlation of -0.543 and R^2=0.295 / 29.5%. It told us that age shared 29.5% of the variability in online shopping. Although age was highly correlated with online shopping according to Spearman's correlation (r=-0.543, sig. =0.000), it still could only explain 29.5% of variation in online shopping. Differently, age shared 17.3% of the variability in internet banking and 12.9% in online education services.

Table 6.8 Summary of Spearman's correlation (r & R^2)

Variables	r	R^2
age vs. usage of online shopping	-0.543	0.295
age vs. usage of internet banking	-0.416	0.173
age vs. usage of online education services	-0.359	0.129
age vs. usage of downloading media	-0.479	0.229
usage of online shopping vs. usage of internet banking	0.586	0.343
usage of online shopping vs. usage of online education services	0.230	0.053
usage of online shopping vs. usage of downloading media	0.388	0.151
usage of internet banking vs. usage of online education services	0.189	0.036
usage of internet banking vs. usage of online downloading media	0.330	0.109
usage of online education services vs. usage of online downloading media	0.337	0.114

6.4 Fraudulent cases

The last three survey questions in section (3) of the questionnaire concerned personal information about actual fraud, attempted fraud and different schemes of attempted fraud. This information is analysed below.

6.4.1 Occurrence of attempted financial fraud (N=271)

The attempted financial fraud we are referring to is the situation in which criminals tried to defraud individuals but have not succeeded in causing monetary loss.

Examples of the mechanisms used include: spam emails, internet hijacking and virus Trojan attacks. 121 out of 271 (44.6%) respondents admitted that they had experienced attempted financial fraud.

The survey instrument contained six measurements to describe the frequency with which individuals perceived that fraud attempts were made on them, namely: Never, Yearly, Quarterly, Monthly, Weekly and Daily. The following table looks at the frequency of occurrence in relation to the seven different but most popular fraud schemes:

Table 6.9 Occurrence of attempted fraud using different schemes

Fraudulent schemes	How often do you experience attempted fraud? (N=271)					
	Never	Yearly	Quarterly	Monthly	Weekly	Daily
Card cloned	94.8%	5.2%	0	0	0	0
ID theft	97.8%	1.5%	0	0.4%	0	0.4%
Scam post / junk mail	65.3%	4.4%	3.7%	9.2%	11.8%	5.5%
Phishing emails / spam emails	62.0%	4.8%	7%	4.4%	13.7%	8.1%
Fake websites / internet hijacking	86.7%	3.3%	3.3%	3.7%	1.5%	1.5%
Lost / stolen bank cards	93.7%	5.9%	0	0.4%	0	0
Virus / Trojan attack	80.8%	8.9%	4.1%	3.3%	1.8%	1.1%

This table has some interesting implications. Looking at the 'never' column first, 97.8% of respondents appear to have never experienced ID theft. Given all the publicity which has been given to this, the incidence of this seems to be surprisingly low. As expected, many respondents had been subject to phishing and spam emails as well a scam post and junk mail, but the incidence of the more technical frauds of virus/Trojan and fake website/internet hijacking seems high (of the order of 20%). Looking now at the frequency of occurrence, card cloning and the loss or theft of bank cards seem to be rare events whereas phishing and scam emails happen on an almost continuous basis. Some of the other schemes seem to vary in frequency with the individual, such as virus/Trojan attacks and fake websites / internet hijacking. This might well be because of the different types of use of the internet by different individuals.

As we look at the correlation between the incidence of virus attack and downloading media online, the statistical results indicated that a positive association discovered (r = 0.203 and Sig. = 0.011). It suggests that certain type of online activities is related to various fraud schemes.

6.4.2 Occurrence of actual financial fraud (N=58)

(1) Summary of real financial fraud

58 out of 271 respondents had experienced actual financial fraud, giving a ratio of fraud occurrence of 21.4%. In monetary terms, the losses suffered from each incidence of fraud ranged from £10 to £7500, with an average of £967.38. As will be discussed later, 91.4% of the defrauded customers received compensation for their loss.

(2) Time series of occurrence of fraudulent cases

In this section, we are looking at the way the 58 fraudulent cases in the survey occurred over time, as depicted in Figure 6.25. The growth pattern is variable, with a small jump in 2000 but a much larger one in 2006.

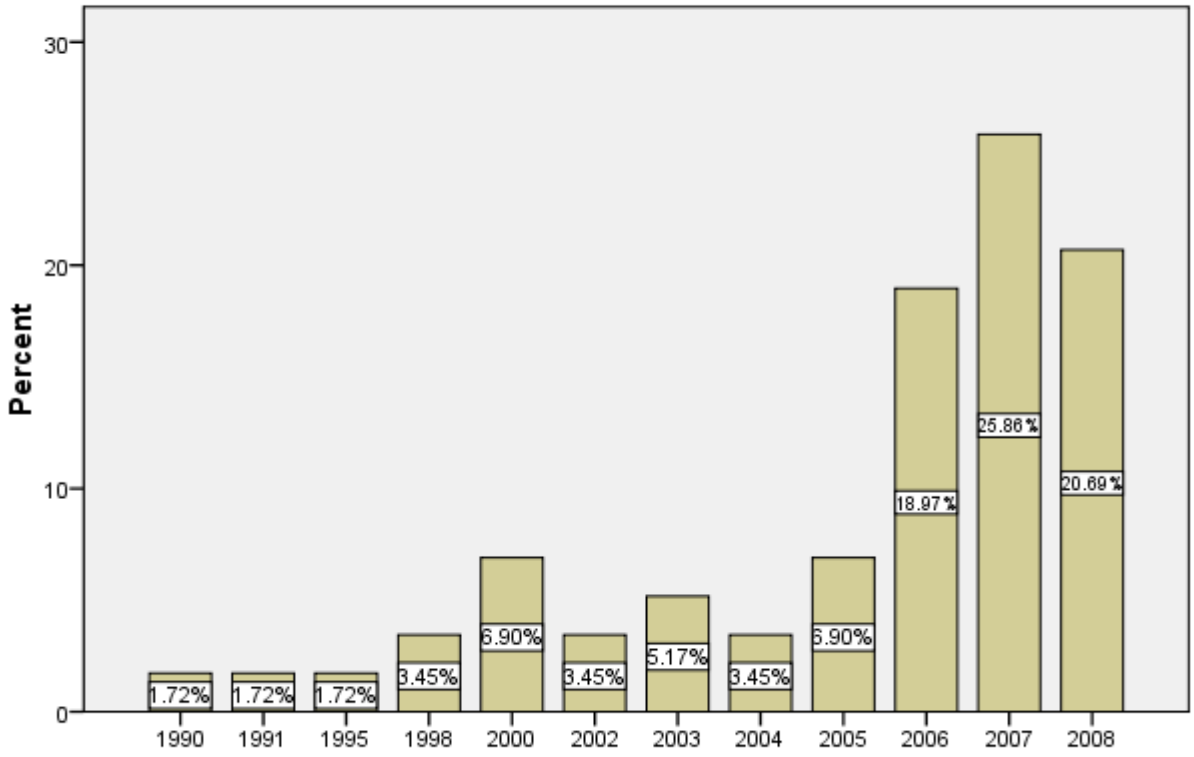


Figure 6.25 Year of fraudulent cases occurrence in the UK

After year 2000, the next turning point is year 2006, in which 11 fraudulent cases occurred, followed by 15 cases in year 2007 and 12 in 2008. The latest fraudulent cases that have been collected occurred in 2008 because the survey questionnaires were sent out in the last quarter of year 2008 and the latest responses have been returned in the first quarter of year 2009.

(3) Fraudulent transactions happen in weekday or weekend

For the 58 cases where fraud had been experienced, 42 replies were received concerning the question: 'when did the fraudulent transaction happen (weekend or weekday)?' In the questionnaire, the day was split into four time periods and then further split by weekday and weekend, giving respondents eight alternatives. It was expected that most fraudulent transactions would take place at the weekend, on the basis that fraudsters would know that the security and vetting systems would be busy

and might be less effective. It turned out that 54.8% fraudulent cases occurred during weekdays and 32.7% at the weekend, however, on a per day rate, this is 11% per day for the five weekdays and 16% per day for the two weekend days, so the weekend rate is higher, although not very much higher as is sometimes presumed. This difference is not significant at the 5% level (z=1.04).

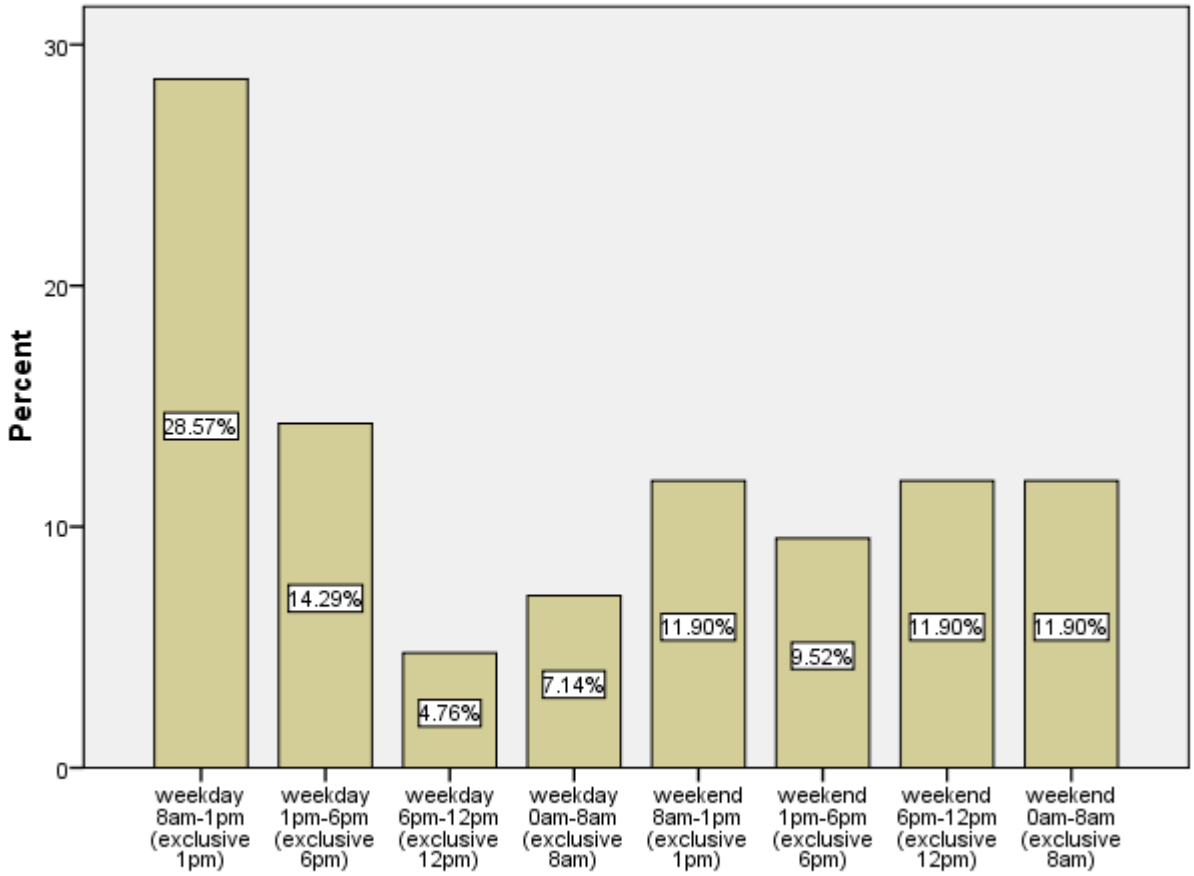


Figure 6.26 Overview of fraudulent transaction occurrence in weekday or weekend

(4) Where does the fraud take place?

With 5 missing values, 53 valid replies were collected about the question: where do you know / believe the fraud took place? 69.8% of respondents believed that the fraud they experienced took place in public places, for example, stations, stores, airports, petrol stations and bars. 22.6% of respondents believed that they were defrauded at home and 7.5% believed that fraud took place in their work place.

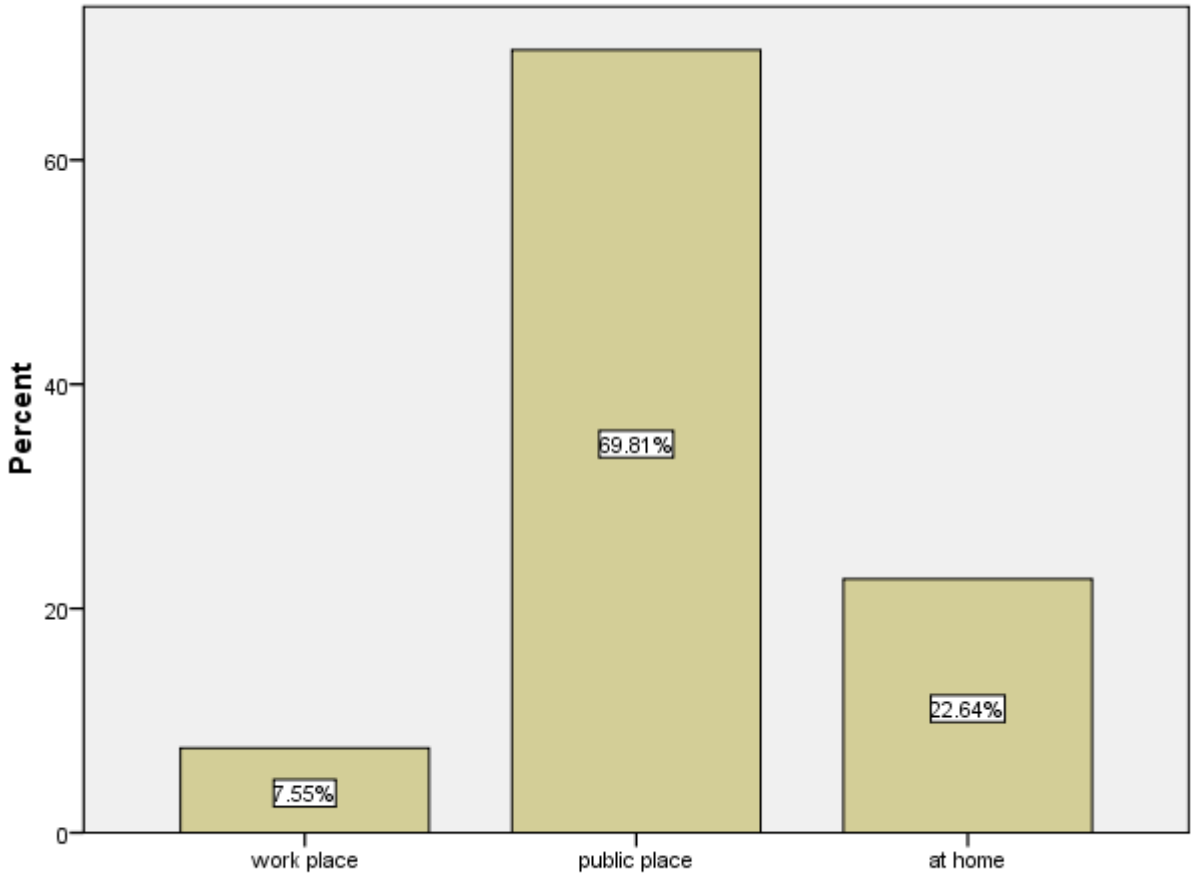


Figure 6.27 Where does the fraud take place?

One explanation for the prevalence of fraudulent activity in public places is the lack of advanced IT support available or installed security techniques. Although internet access is provided in many stations, airports, cafes / restaurants, there is no guarantee of IT security. Even though individuals are aware of the potential risks, the importance of getting online access outweighs the risk. In addition, the individual might be in a hurry and willing to 'cut corners' to get access without ensuring that security measures are in place.

The other explanation is that individuals are more easily distracted in the public places than a place they are more familiar with, such as work place and home. When someone is sitting in the waiting lounge in the airport, he or she has no idea who is

sharing internet access; which network security techniques have been applied and whether or not there is any updated security support.

(5) How soon after the fraud was discovered?

With 58 replies in total, 36 replies fell into the three most popular categories, which are: within 7 days, within 24 hours and within 12 hours. The following table gives a breakdown across all the categories and the figure shows these in diagrammatic form.

Table 6.10 How soon after the fraud was discovered?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	within 12 hours	10	17.2	17.2	17.2
	within 24 hours	11	19.0	19.0	36.2
	within 7 days	15	25.9	25.9	62.1
	2 weeks later	9	15.5	15.5	77.6
	4 weeks later	9	15.5	15.5	93.1
	more than 1 month	4	6.9	6.9	100.0
	Total	58	100.0	100.0	

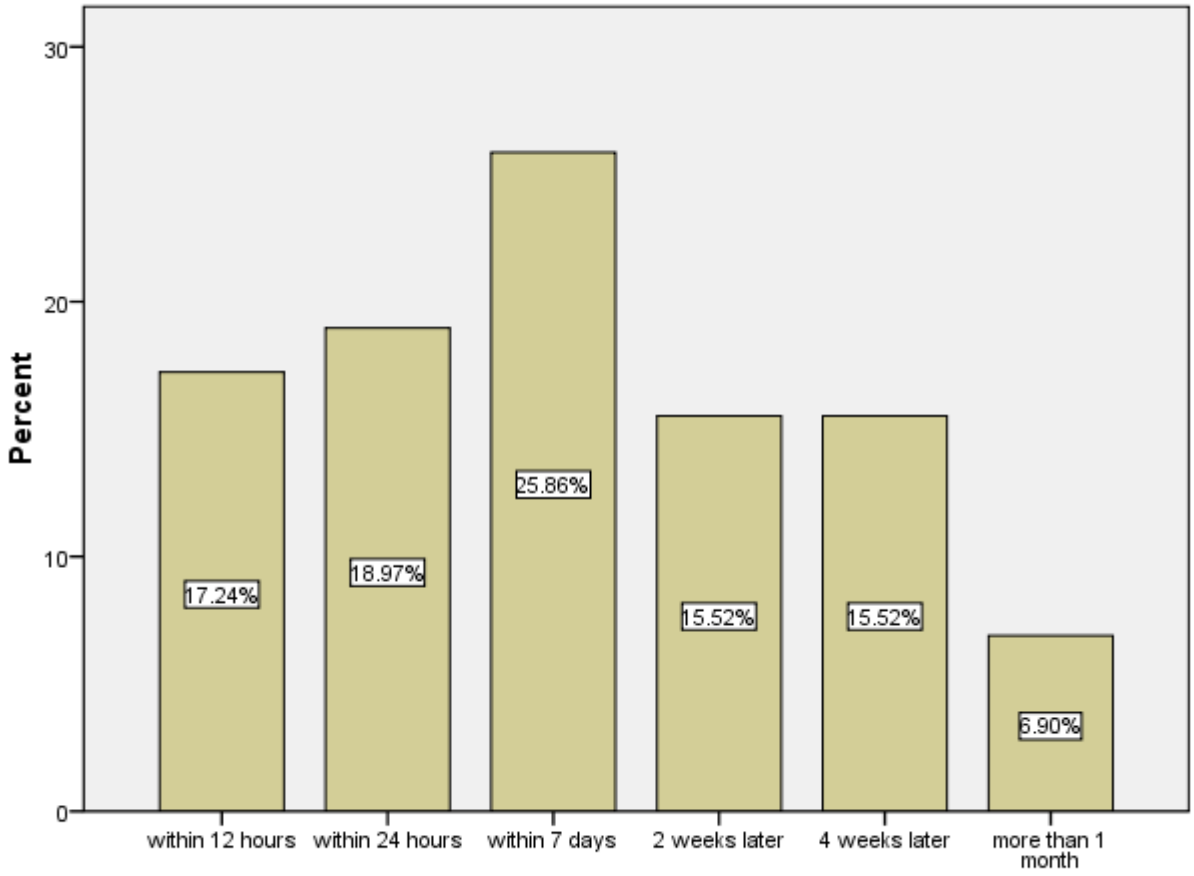


Figure 6.28 How soon after the fraud was discovered?

Subsequently (Figure 6.30) it is seen that most of the frauds involve credit cards. In interpreting Figure 6.28, it is therefore likely that the frauds that are discovered quickly are likely to be the result of checks by the credit card companies (eg in detecting unusual patterns of use), whereas those detected in the medium to long terms are more likely to be customer detected as a result of the customer checking his/her statement. Since the statement can arrive anytime up to four weeks after the fraudulent transaction, the pattern of customer detection is likely to occur evenly over time as appears to be reflected in the diagram. Also consistent with this rationalisation is that the proportion of frauds (7%) detected more than a month after occurrence is fairly low.

A key factor in early detection of fraud is the increasing sophistication of the monitoring of financial transactions by banks and credit card companies – this not only helps to reduce financial loss but gives the customers more confidence and enhances the reputation of the financial companies, who can use modern technology (mobile phones, the internet etc) to contact customers quickly if they note any suspicious activity.

(6) Which type of fraud scheme was used?

In section 6.4.1, attempted fraud was discussed. Here we concentrate on actual fraud as evidenced by the 58 respondents who had experienced it, the alternatives listed in the survey being: phishing email / spam emails; fake websites / internet hijacking; virus / Trojans; lost / stolen bank cards; card clone and card ID theft. In addition, we provided blank space for respondent to fill in any other information if necessary. Surprisingly, none of the 58 respondents was defrauded by phishing emails / spam emails which suggests that respondents are wise to this form of deception.

The main fraud schemes encountered by the 58 respondents who have experienced actual fraud were: card cloned, card ID theft and lost-and-stolen card. 23 out of 58 respondents (39.7%) experienced card clone fraud (which is also called counterfeit card fraud). 21 out of 58 respondents (36.2%) who experienced actual fraud were caught out by card ID theft. 17.2% respondents have been defrauded due to lost-and-stolen card fraud. Figure 6.29 below shows the breakdown into these categories.

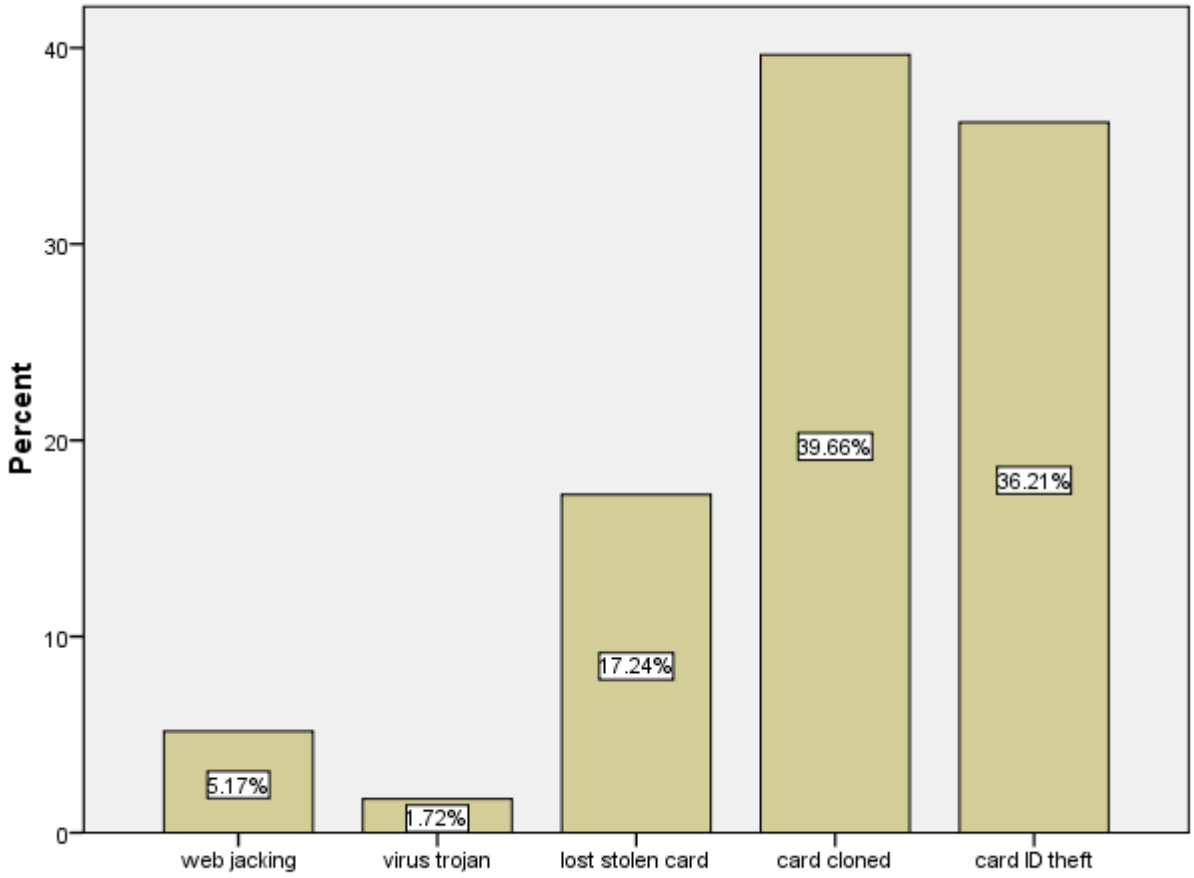


Figure 6.29 Which type of fraud scheme was used?

(7) Which type of payment method was used in this case?

Five options for payment method were listed for the question asking for the payment method used for the fraud. These were: credit card; debit card; pre-paid card; cheque and secure internet payment (e.g. PayPal). Also we offered blank space to respondents to add anything they would like to. There were 2 missing values giving 56 valid replies.

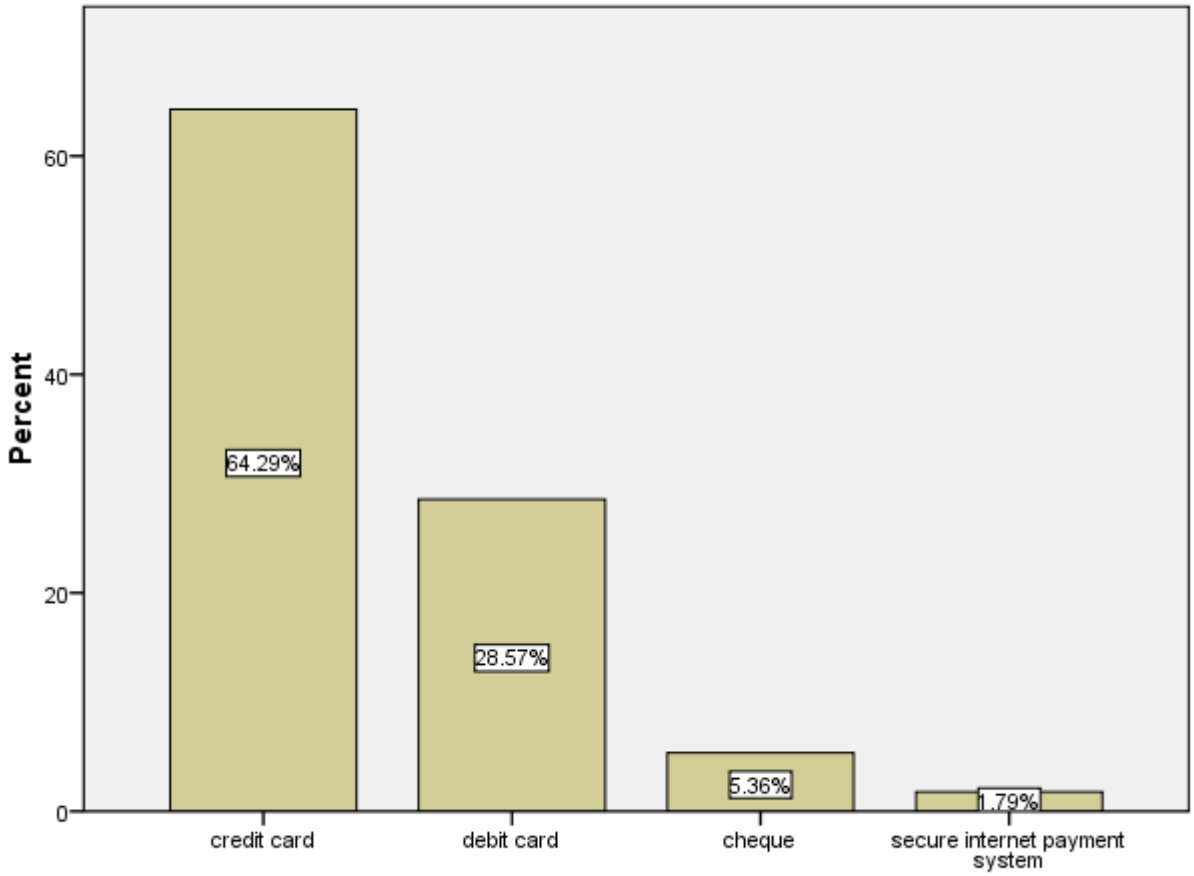


Figure 6.30 Which type of payment method was used?

The breakdown is shown in the following table. Almost two thirds of the frauds involved credit cards, which partly reflects the greater usage of credit cards but also their greater vulnerability, as debit cards are directly linked with an individual's bank account and will not allow spending that take the balance of the account beyond preset limits.

As stated in the report of 'card expenditure statistics (The UK Cards Association 2010)' in January 2010, the total spending in the UK on all plastic cards was £ 31.1 billion, of which debit cards spending was £ 21.1 billion and credit cards spending was £ 9.9 billion, the remaining £0.1 billion being on pre-pay and charge cards.

Table 6.11 Which type of payment methods was used in this case?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	credit card	36	62.1	64.3	64.3
	debit card	16	27.6	28.6	92.9
	cheque	3	5.2	5.4	98.2
	secure internet payment system	1	1.7	1.8	100.0
	Total	56	96.6	100.0	
Missing	99	2	3.4		
Total		58	100.0		

However, the credit cards (£60-65) beat the debit cards (£40-45) on the average transaction values in the UK (The UK Cards Association 2010). On the other hand, 48% of the card payment on the internet was made by debit card and 52% by credit or charge cards (The UK Cards Association 2010). As supported our findings in Table 6.11, the individuals would prefer credit card to debit card when they make payment on the internet.

(8) Did any parties compensate you?

We received 57 valid replies to the question asking whether or not defrauded individuals got any compensation. 53 respondents (91.4%) got compensation from the bank / credit card company and two respondents got compensation from the merchant instead. The other two respondents did not get any compensation.

On the evidence of the survey questionnaire, in general it is the banks / credit card companies that bear the losses of financial fraud. Once the fraudulent cases have been reported, the financial organizations deal with it on behalf of defrauded customers. Unless the evidence showed that customers were involved into fraudulent cases on purpose, refund / compensation will be arranged to individuals, normally by reversal of the fraudulent transactions on the financial statements.

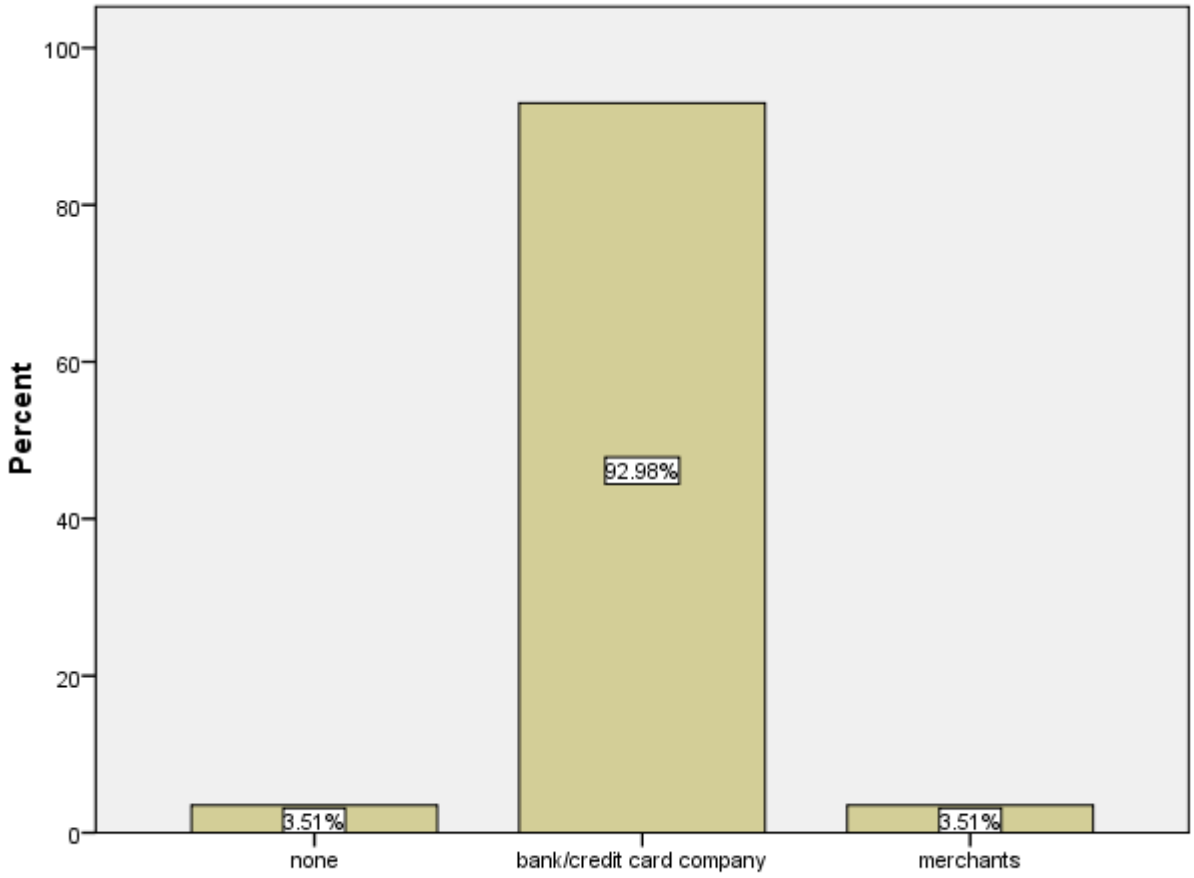


Figure 6.31 Did any parties compensate you

It is not always the banks / credit card companies that bear the losses in the fraudulent cases, particularly where online financial transactions are involved. The credit card companies have the right not to pay the merchants if there have been procedural irregularities – for example if the requisite checks and authorizations have not been carried out. However, it is generally the banks/credit card companies that bear the loss.

Given the increasing level of financial fraud, how can the banks/credit card companies afford to bear the cost involved? As discussed in chapter 3, section 3.3, credit card operations make their money in approximately equal amounts from the merchant fees charged and on the interest earned from customers who do not pay off their balances every month. The rate of interest on credit cards can vary from around 9% to over 29%, and with money being available on the wholesale markets at around 2%, there is

clearly a massive default premium built into the rates charged to customers. For any credit card company, a key driver in the financial model is the number of transactions, and it is in the company's interest to keep customers happy and to keep using the card. Settling fraud cases quickly, and in the customer's favour, helps to achieve this. This issue of satisfaction is measured in (10) below.

(9) Awareness of different type of financial fraud

We used five scales (from 1 to 5) to measure the degree of awareness of types of financial fraud. 26 out of 58 defrauded respondents (44.8%) scored average to describe their awareness of types of financial fraud. 36.2% respondents who have been defrauded ticked two scales below average to their awareness of types of financial fraud and 18.9% ticked two scales beyond average on this question. This is a subjective question as each individual will have different ideas about what constitutes, for example, 'average' awareness, but it is of interest to see how the individuals who have suffered fraud rate their own awareness.

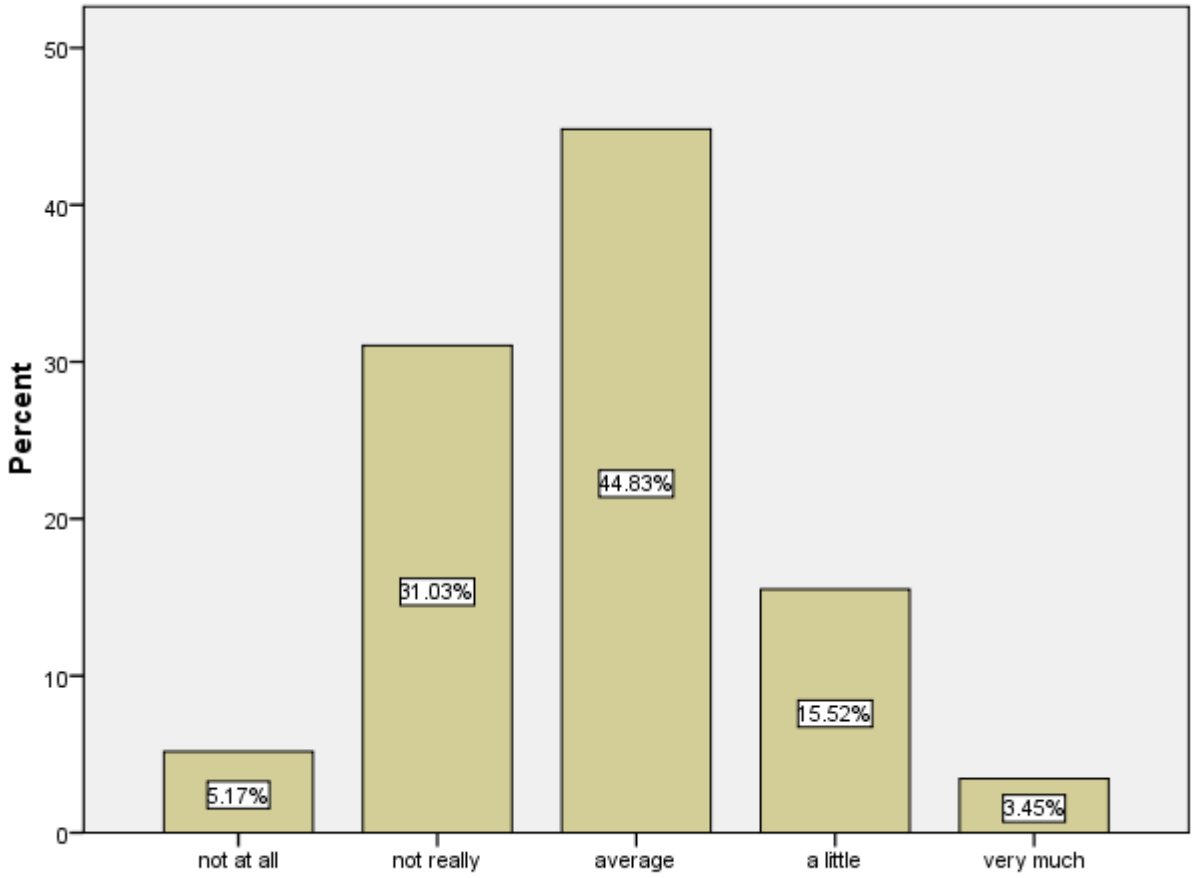


Figure 6.32 Awareness of different type of financial fraud

As suggested by the figure below, most individuals who have experienced actual fraud are aware of financial fraud, particularly for online financial transactions. 44.8% respondents believed that their awareness of the fraud is average and 18.9% even beyond average. But there were still 36.2% respondents who have experienced actual fraud admitted that they are not really aware of the different types of fraud. Since the banks / credit card companies step in to try to resolve the situations once the fraudulent transactions occur, this appears to make some individuals rather complacent. As with moral hazard in the insurance industry, business organizations have to take certain risks, even pay for the increased costs caused by a small group of customers. Moral hazard arises from asymmetric information, in this instance from the fact that the bank does not know which of its customers are lax in terms of security and therefore there is no uniformity of risk. According to Holmström (1979), a first

best solution is only provided by the monitoring of the actions of individuals, which would be prohibitively expensive, but could be proxied by a contract that contains forcing terms that induce better behaviour. For example, banks will not reimburse customers if the fraud is caused by certain types of injudicious actions, such as when a customer loses a wallet which contains both a credit card and a note of the associated PIN number. In this case, the bank is likely to refuse to reimburse the customer should fraudulent use of the credit card ensue.

(10) How satisfied with bank/ credit card company in dealing with fraud

Considering the refund / compensation arranged by banks / credit card companies, our expectation is that individuals who have experienced fraud are more likely to feel satisfied with banks / credit card companies. Not surprisingly, the figures and bar chart are compatible with our assumption about the defrauded customers' satisfaction with the financial organizations in dealing with fraud.

With 1 missing value, 57 valid answers were collected. 54 out of 57 respondents (94.7%) responded that their satisfaction level was at least average, with 32 of these indicating a higher than average level of satisfaction. There would therefore appear to be a general level of satisfaction with banks / credit card companies in dealing with fraud. Possible reasons for this have already been advanced in (8) above.

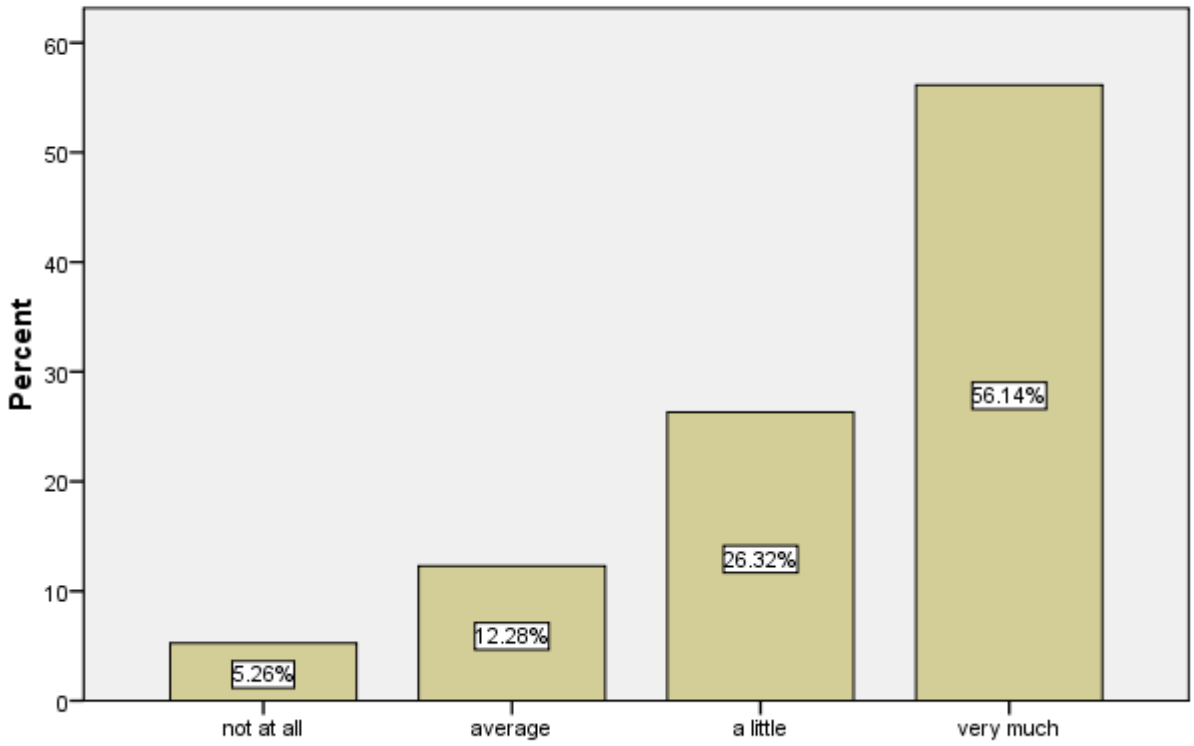


Figure 6.33 How satisfied with bank / credit card company in dealing with fraud

However, three of the 57 respondents (5.3%) were not satisfied at all with the banks / credit card companies in dealing with fraud. In the previous section discussing whether the defrauded individuals get any refund / compensation, we found that two respondents have not got any refund / compensation. On that case, we can understand why the respondents gave the lowest score to describe the satisfactions with the banks / credit card companies in dealing with fraud because the individuals had to bear the financial losses themselves.

6.5 Fraud occurrence model (N=271)

In this section, we are trying to build up a model to explain and predict fraud occurrence based on the associations and correlations between different variables.

6.5.1 Tests for associations and correlations

We begin our more formal testing by looking at the association between pairs of variables to get a better understanding of the responses. In some cases we are looking at the correlation between the explanatory variables to explore the extent to which they are multicollinear, but generally we are looking at associations between the incidence of fraud (which is the main variable we are trying to explain) and the other variables in the survey. To accomplish this we use a Chi-square (χ^2) test to test the association, although we could also have used an F-test.

The following table shows the Chi-square test results including Chi-square value, sig. value, and explanations based on the results. We use three examples to explain the table in details: firstly, we look at the row starting with general IT skills vs. fraud occurrence (Chi-square value = 9.024; Sig. = 0.011; r = 0.168 and sig. = 0.004). This suggests that there is a positive and significant relationship between general IT skill and fraud occurrence, which is an interesting finding, implying that although one would expect those with better IT skills to make more intensive use of the internet, their skills do not make them immune from fraud.

The Chi-square test concerning the association between age and fraud occurrence (Chi-square value = 6.663; Sig. = 0.036; r = -0.108 and sig. = 0.076) is telling a different story. The r value is negative, suggesting that older people are less likely to experience fraud, but the correlation is not significant at the 5% level.

We could not discover any significant association between education background (IT / Finance related) and fraud occurrence (Sig. = 0.882 / 0.839). It was initially suggested that respondents who had an education background in either IT or Finance might have an advantage in avoiding financial fraud on the internet, but this was not supported by the data.

Table 6.12 Chi-square tests					
Variables	**Value****	**Sig** different from zero	**r**	**Sig** different from zero	**Implication**
General IT skill* vs. Age	1.015E2	0.000	-.601	0.000	Younger respondents are more likely to have higher general IT skill
General IT skill vs. Fraud occurrence	9.024	0.011	0.168	0.004	Respondents with higher general IT skill are more likely to be defrauded on the internet
General IT skill vs. Highest qualification	44.085	0.000	0.202	0.001	Respondents with higher qualification are more likely to have higher IT skills
Age* vs. Fraud occurrence	6.663	0.036	0.108	0.076	Younger respondents are more likely to be defrauded on the internet
Usage of internet banking vs. Fraud occurrence	12.532	0.000	0.215	0.000	Respondents who are using internet banking are more likely to be defrauded on the internet
Usage of online shopping vs. Fraud occurrence	12.140	0.000	0.212	0.000	Respondents who are using online shopping are more likely to be defrauded on the internet
Usage of downloading media vs. Fraud occurrence	11.936	0.001	0.210	0.001	Respondents who are using media download are more likely to be defrauded on the internet
Usage of online education vs. Fraud occurrence	0.767	0.381	0.053	0.383	No significant relationship was found
IT/Finance related background vs. Fraud occurrence	0.661	0.882	0.012	0.839	No significant relationship was found
General IT skill vs. Gender	8.214	0.223	0.106	0.082	No significant relationship was found
Gender vs. Fraud occurrence	2.562	0.109	0.097	0.110	No significant relationship was found
Highest qualification vs. Fraud occurrence	8.284	0.040	0.097	0.109	No significant relationship was found
*variable has been combined and recoded to avoid inaccurate test result (e.g. Age/IT skill) **value is referring Chi-square value.					

6.5.2 Logistic regression model

In this section we are trying to build up a model to explain the propensity for individuals to be subjected to financial fraud. The dependent variable is therefore a limited dependent variable (LDV) or categorical variable which takes on the values zero or one depending on whether fraud has been experienced or not. According to Field, A. (2009, p265), logistic regression is multiple regression but with an outcome variable that is a categorical variable and predictor variables that are continuous or categorical. Similarly, the outcome variable of the model we are trying to build up is to predict fraud occurrence which is a binary variable, e.g. fraud occurrence=1; no fraud occurrence=0. Assumed predictor variables might be categorical (e.g. usage of gender / age) and numerical data (e.g. history of credit card usage).

Based on the association and correlation table in the previous section, we use 11 predictors including categorical and numerical variables to run a logistic regression. SPSS has more than one approach to test logistic regression. We chose an approach referred as 'Forward LR' by Field, A. (2009, p283) in which variables are added to the logistic equation in the order of the significance of their binary relationship with the dependent variable. The following two stages describe the progress of Forward LR test in details:

(1) Beginning block

At this stage, the initial model originates from using only the constant in the regression and tells us about the basic model included constant only. -2LL (-2 Log likelihood) in the following table represents the fit of the basic model to the data. Field, A. (2009, p283) addressed: 'when including only the constant, the SPSS bases the model on assigning every participant to a single category of the outcome variable'. In our study, SPSS can decide either to predict that the fraud occurrence or fraud not occurrence.

Table 6.13 Iteration history

Iteration History[a,b,c]			
Iteration		-2 Log likelihood	Coefficients
			Constant
Step 0	1	241.731	-1.023
	2	241.269	-1.127
	3	241.268	-1.130
	4	241.268	-1.130

a. Constant is included in the model.
b. Initial -2 Log Likelihood: 241.268
c. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Indicated by Field, A. (2009, p283), SPSS will predict every case into the category into which most observed cases fell. In the Classification table below, there are 164 cases representing no occurrence of fraud and 53 cases representing occurrence. The chance of fraud occurrence is 53/164+53=24.4% and the chance of fraud not occurrence is 164/164+53=75.6%. In this simple model, with only a constant, SPSS predicts that all cases are representing the non-occurrence of fraud as this gives a higher percentage of correct classifications (100 / 0). As expected, this initial model correctly classified 75.6% cases.

Table 6.14 Classification table

Classification Table[a,b]					
	Observed		Predicted		
			fraud occurrence or not		
			not occurrence	occurrence	Percentage Correct
Step 0	fraud occurrence or not	not occurrence	164	0	100.0
		occurrence	53	0	.0
		Overall Percentage			75.6

a. Constant is included in the model.
b. The cut value is .500

The 'variables in the equation' table below summarizes the model and shows the

value of the constant (b_0), which is equal to -1.130.

Table 6.15 Variables in the equation

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 0	Constant	-1.130	.158	51.108	1	.000	.323

Where B is the coefficient of the predictor variable, S.E (standard error), the standard deviation of the sampling distribution of a statistic (in this case the coefficient B), Wald is a test statistic with a known probability distribution that is used to test whether the B coefficient for a predictor in a logistic regression model is significantly different from zero, df is the degrees of freedom (essentially, the number of 'entities' that are free to vary when estimating some kind of statistical parameter), Sig is the significance value expressed as a tail probability, and Exp(B) is the odds ratio, which is an indicator of the change in odds resulting from a unit change in the predictor in logistic regression; if the value is greater than 1 then it indicates that as the predictor increases, the odds of the outcome occurring increase. Conversely, a value less than 1 indicates that as the predictor increases, the odds of the outcome occurring decrease.

Before proceeding, we present a table of variable definitions for variables used in the next stage of the analysis.

Table 6.16 Full name of the variables

NEWITSKILL	IT skills
NEWAGE	Age
NEWHIQUALI	Highest qualification
GENDER	Gender
UOOAOS	Usage of online shopping
UOOAIB	Usage of internet banking
UOOAOES	Usage of online education services
UOOADM	Usage of online media downloading
EBG	Education background
HUCC	History of usage of credit card
HUDC	History of usage of debit card

In the 'variables **not** in the equation' table, we need to focus on column sig and column score. For example, UOOADM (usage of online downloading media) has the sig. value as 0.003, which suggested variable UOOADM would make a significant affect to the model if it is included in the test. UOOADM also has the highest score value as 8.724, which would make a potential contribution to the model. Considering a significant score value, variable UOOADM is likely to be a good predictor. In the next iteration, this variable is added to the logistic equation.

Table 6.17 Variables not in the equation

Variables not in the Equation

			Score	df	Sig.
Step 0	Variables	NEWITSKILL	6.921	1	.009
		NEWAGE	1.777	1	.183
		NEWHIQUALI	.981	1	.322
		GENDER	2.187	1	.139
		UOOAOS	8.089	1	.004
		UOOAIB	8.458	1	.004
		UOOAOES	1.878	1	.171
		UOOADM	8.724	1	.003
		EBG	.067	1	.796
		HUCC	.054	1	.816
		HUDC	8.245	1	.004
		Overall Statistics	33.719	11	.000

(2) Forward LR Procedure

Now we are looking at an improved model which is different from the basic model we were discussing in previous section. This procedure is repeated, with SPSS adding variables into the logistic regression one by one, on the basis of the strength of their statistical association with the dependent variable, in order to create an improved model. This is continued until the point where adding additional variables does not add statistical significance to the model.

Continuing with our example, the model summary table below shows the overall fit of the new model through four iterations. The -2LL value of this new model has decreased from 232.927 at step 1 to 209.158 at step 4, this being less than 241.268 which was the value of -2LL in the previous basic model, showing that the model is predicting the outcome variable more accurately.

Table 6.18 Model summary (forward LR)

Model Summary			
Step (iteration)	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	232.927[a]	.038	.056
2	221.902[b]	.085	.127
3	216.284[b]	.109	.162
4	209.158[b]	.138	.205

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.
b. Estimation terminated at iteration number 5 because parameter estimates changed by less than .001.

Also, when we look at the Chi-square test table originated from the new model, we noticed that all the sig. values are less than 0.05. It suggests that the overall model predicts fraud occurrence or non-occurrence significantly better than when only the constant was included.

Table 6.19 Tests of model coefficients (forward LR)

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 4	Step	7.126	1	.008
	Block	32.111	4	.000
	Model	32.111	4	.000

Similarly to the basic model in previous section, the classification table describes how well the model classifies the cases overall. The basic model with only a constant could classify 75.6% cases but with other predictors included in this new model, we can classify more cases raised to 78.3%.

Table 6.20 Classification table (forward LR)

Classification Table[a]

Observed			Predicted		
			fraud occurrence or not		
			not occurrence	occurrence	Percentage Correct
Step 4	fraud occurrence or not	not occurrence	158	6	96.3
		occurrence	41	12	22.6
		Overall Percentage			78.3

a. The cut value is .500

Now we are focusing on the table of variables in the equation. In this table, we can get the estimates for the coefficients for the predictors included in the model. For example, at the step 1, variable UOOADM is added into the model to predict fraud occurrence or not. The coefficient of UOOADM is 0.953 and its sig. value is 0.004 which is significant. It suggested that variable UOOADM is a good predictor in the model. With the coefficient of the constant is -1.472 at step 1, we can format the equation of the step 1 model.

Finally, we need to explain the last crucial value in the table of variables in the equation. Exp (B), generally speaking, it suggests a positive relationship between predictor and outcome if the value is greater than 1. On the other hand, a negative relationship occurs when the value is less than 1. One of the predictors at the step 4, UOOAOES (usage of online education service), has the value of Exp (B) =0.327 which is less than 1. Also, the coefficient of UOOAOES is -1.117 suggesting a negative relationship between UOOAOES and fraud occurrence.

Based on the best model selected by SPSS using logistic regression test, we have four predictors with significant performance: UOOAIB (usage of internet banking), UOOAOES (usage of online education service), UOOADM (usage of online downloading media) and HUDC (history of debit card usage). Except for a negative

relationship shown by UOOAOES, the other three predictors have a positive relationship with fraud occurrence.

Table 6.21 Variables in the equation (forward LR)

Variables in the Equation									
								95.0% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	UOOADM	.953	.328	8.432	1	.004	2.594	1.363	4.935
	Constant	-1.472	.210	49.333	1	.000	.230		
Step 2[b]	UOOADM	1.152	.347	11.036	1	.001	3.163	1.603	6.240
	HUDC	.063	.020	10.479	1	.001	1.065	1.025	1.107
	Constant	-2.772	.479	33.457	1	.000	.063		
Step 3[c]	UOOAIB	.918	.405	5.145	1	.023	2.505	1.133	5.539
	UOOADM	1.005	.355	8.010	1	.005	2.733	1.362	5.484
	HUDC	.064	.020	10.245	1	.001	1.066	1.025	1.109
	Constant	-3.401	.589	33.338	1	.000	.033		
Step 4[d]	UOOAIB	1.069	.418	6.548	1	.010	2.911	1.284	6.600
	UOOAOES	-1.117	.441	6.423	1	.011	.327	.138	.776
	UOOADM	1.345	.389	11.943	1	.001	3.839	1.790	8.232
	HUDC	.063	.020	9.687	1	.002	1.065	1.024	1.109
	Constant	-3.327	.603	30.465	1	.000	.036		

a. Variable(s) entered on step 1: UOOADM. b. Variable(s) entered on step 2: HUDC.
c. Variable(s) entered on step 3: UOOAIB. d. Variable(s) entered on step 4: UOOAOES.

The implications of the results are as follows. They suggest that usage of internet banking, the extent of downloading media from the internet and history of usage of debit cards are all positively associated with the incidence of fraud occurrence, whereas interestingly the usage of online educational services is negatively related to the occurrence of internet fraud. This last finding might reflect the possibility that educational websites are 'safer', or possibility that those who are interested in education are more knowledgeable and have a tendency to avoid situations in which fraud might occur. Interestingly, this result might not appear to sit easily with the finding in section 6.3-(4)-4.1 that individuals with higher degrees were more susceptible to fraud, but an explanation is that frauds experienced by those with higher qualifications were not incurred as the result of downloading educational material.

6.6 Conclusions

In this chapter, we have undertaken a progressive analysis of the UK survey data obtained, starting first with a descriptive approach, then looking at binary associations of the variables and then using logistic regression to try to explain and classify the occurrence of fraud. The results from the logistic regression suggest that certain internet related activities, such as internet banking, downloading of media and history of debit card usage are all positively associated with the occurrence of fraud, whereas the use of online educational services is negatively related. Interestingly, on-line shopping, which was significant in the univariate analysis as evidenced by the chi-square test, was not significant in the logistic regression.

Chapter 7 Financial Payments Systems in China

7.1 Introduction

The purpose of this chapter is to provide an introduction to the credit card, debit card and online transactions environment in China as a prelude to analyse the results of the China survey in chapter 8.

7.2 Credit cards / debit cards service in China

7.2.1 Overview of credit / debit card in China

From the invention of money (allegedly by the Phoenicians), there have been a number of significant milestones in the form it takes, eg in the transition from precious metals to base metals to paper notes. In the mid-20 century, some merchants and restaurants started to issue store cards to trustworthy customers to provide them with an alternative method of payment, subject to terms agreed between the customer and the merchant. Periodically, customers would be provided with a statement in the form of a note or list posted by each merchant. No interest would be charged if customers paid off the amount due on time, otherwise interest would be charged at an agreed rate. These store cards not only brought additional convenience to customers but also helped merchants to promote their businesses.

This practice led to the next major evolution in the development of money. In 1950[7], Diners' Club cards were launched as the very first credit card (Liu 2008). Card holders became club members first and agreed to pay an annual fee / service charge to the club as well as paying for the transactions. More advanced than the store card mentioned above, Diners' Club cards could be accepted by other merchants outside the club. This advantageous payment method attracted the attention of many financial

[7]The Diners Club Card was the first ever Charge Card. In 1950, businessman Frank McNamara entertained a group of dinner guests in a New York restaurant, only to discover that he'd forgotten his wallet. Luckily, the restaurant owner knew him and let him leave his business card as an IOU. This inspired McNamara to devise a card to prove the holder's identity and ability to pay. He launched the Diners Club Card that year and the initial membership was 200 with the card being accepted in 27 restaurants. In 2008, there are 8 million Diners Club Cardholders in over 200 countries, and the card is accepted in 6 million establishments worldwide.(Diners Club website).

organizations. Two years later, T&E (Travel and Entertainment Inc.) entered the market and rapidly built up its business. In 1966, the bank card system arrived in Europe with the introduction of Barclaycard in the UK (Liu 2008).

A bank card service is still a new concept for Chinese people who have been used to cash transactions for generations. The development of bank cards has been through three identifiable stages in China:

(1) From 1978 to 1993

Since the reform and open policies were launched in 1978, China was committed to seeking more international connections. In 1979, the Bank of China, Guangdong branch, entered into the bank card industry by cooperating with the Bank of East Asia. In the following 15 years, the big four state-owned banks in China consisting of the Bank of China, the Industrial and Commercial Bank of China, the China Construction Bank and the Agricultural Bank of China started to build up their own bank card programme and each joined one or both of the two major credit-card clearing operations – either Visa International or MasterCard.

At this early stage, each bank set up its own bank-card standards and policies. With little experience to draw on, banks were unable to provide a quality service or properly functioning products and in addition bank-cards were only valid within a given geographical area, not even nationwide. With these inconveniences, the demand for bank-cards was limited and cash was still the prime payment method in China.

(2) From 1994 to 2001

Having gone through a 15 year period of preparation, the bank-card industry in China was ready for the next stage of development. In 1994, the central bank (the People's bank of China) started to standardize the Bank-card industry by introducing a standard practice code, a nationwide network, POS/ATM equipment, information exchange and other services. From the end of 1998, bank cards became usable on a nationwide basis.

With these improvements, bank-cards, particular debit cards, started to attract two groups of individuals in China: professionals and students. Debit cards reduce the risk

of cash carry and allow individuals to withdraw or deposit cash 24/7 using an ATM. As more ATMs were installed and self-service bank branches opened, more customers were willing to use debit cards.

(3) From 2002 to the present

In March 2002, China Unionpay (CUP) was established in Shanghai under the approval of the People's Bank of China as the sole bank card association. Playing the role of the regulator of the bank-card industry in China, CUP takes responsibilities for development of the bank-card industry and the improvement of operating systems. Using standards and regulations, CUP helps to manage cross-border transactions and data processing.

Through these three development stages, the bank-card system has been established in China to international standards. Consumers have started to accept and to get used to modern financial products and services, but Chinese consumers have been more willing to subscribe for debit cards than credit cards, reflecting Chinese tradition and culture lasting for thousands of years.

7.2.2 Credit card vs. debit card in China

Following the three development stages of the bank-cards industry in China, by June 2006 the sum of issued bank cards reached twice the figure in 2001 (Liu 2008). Of all the bank cards issued in 2001, 95% are debit cards (People's Bank of China).

Table 7.1 Debit cards and Credit cards issued in China 2007-2009[8] (m = million)

	Year 2007	Year 2008	Year 2009
Debit cards	752.3 m	1003 m	1180 m
Credit cards	126.2m	140.2 m	187 m

The Table 7.1 shows clearly that credit cards constitute an increasing but still small proportion (about 12-14%) of the bank-cards issued in China from 2007-2009. The tradition of paying by cash and an aversion to borrowing money appear to the main

[8] Source: from a professional working in the financial industry in China, 2010.

reasons for this, rather than any institutional or regulatory factors (such as, for example, restrictions on the granting of credit). Overspending and living on debt are regarded as shameful behaviour, even crimes in Chinese traditional culture, which sings high praise for being moderate and exercising self-discipline. One of the very important lectures to children is 'spend less and save more'. Individuals are supposed to be proud of how much they have saved not spent. Overspending is considered bad behaviour which would compromise an individual's reputation and family standing.

As well as the influences of Chinese traditional culture, in the more recent history of China, in particular the last 100 years, Chinese people have struggled for generations against invasions, wars and natural disasters which almost proved to be catastrophic. Having been through these tough periods, Chinese people try to prepare for the future by saving and not spending.

7.2.3 Credit card / debit card fraud in China

It is easy to find out that any innovations in human history always come along with risks and compromises in consequence. Mobile phones make communication easier and quicker but at the cost of privacy. In replacing cash as a popular payment solution, bank cards bring convenience to consumers but create a new type of financial fraud: bank card fraud.

Card fraud is just starting to be a significant development in China. Based on the Chinese survey results we obtained, 7 out of 142 respondents (4.9%) experienced actual fraud compared to 58 out of 271 in the UK (21.4%). The explanation of the low fraud rate in China comes from two aspects: firstly, the card holders in China are very well educated, as we can see from the survey results, with 86% holding a degree. In consequence, 87.3% of respondents had IT skills of average or better. Secondly, the bank-card is still new to China and criminals are still learning to exploit the vulnerabilities of the system.

According to the findings based on the fraudulent cases in the recent three years (Zhang, Luo 2009), 87.2% are lost-and-stolen card fraud. In contrast to the UK, credit card holders are allowed to choose either a signature or a PIN number to verify transactions in China. Criminals can forge a signature to purchase products in person from retailers until the original card holder reports that the credit card is lost. Debit cards are not affected in this way because only PIN usage is allowed to verify debit card transactions in China. Lost-and-stolen card fraud cannot be conducted online in China because online shopping is limited to settlement by online banking transactions only.

Except for lost-and-stolen credit card fraud, which accounts for 87.2% of fraudulent credit card transactions, there are three other main types of credit card fraud in China currently:

(1) ID theft (Zhang, Luo 2009), which is in essence the same as it is in the UK, whereby criminals apply for credit cards using someone's ID illegally. With this type of fraud, criminals can even can set PIN numbers and withdraw cash from an ATM instead of making purchases.

(2) Card cloning, which is again essentially the same activity as experienced in the UK, whereby criminals make a copy of the authentic credit / debit cards illegally. All bank cards currently in usage in China, just like the old version of bank cards in the UK, only have a magnet strip on the back. It is easy to have bank cards cloned without a chip embedded providing further security protection. In particular, some malicious cashiers even steal and sell customers' bank cards information using an illegal card reader.

(3) Collusion (Zhang, Luo 2009), either original card holders or fake card holders can collude with merchants to make false transactions and split the cash obtained. It is not difficult for merchants to purchase the POS equipment which is used to make card transactions.

Debit card fraud is very rare in China because PIN usage is the only way to verify transactions and identify card holders since the first debit card launched into Chinese market. For online shopping, all bank cards have to be operated using online banking procedures to make payments on the internet. As was established in the interviews with banking officials, normally banks do not take any responsibility for debit card fraud / loss in China – this in itself is likely to make individuals more cautious.

7.2.4 Credit card / debit fraud cases in China

In this section, we paraphrase some cases of credit card fraud from examples given in the Chinese banking literature.

Case 1 (Wang 2004, p90):
25th, January 1997, Mr. H applied for a credit card from a local bank providing a false employment letter and a false income certificate. Within one week, H made several purchases in shopping malls and obtained cash by faking transactions in collusion with illegal merchants. The total loss incurred was 38,000 RMB (about £3,800) up to the time when H was traced and arrested in Luo Yang city.

This case (and other similar ones that are not discussed here) exposed that how weak the personal credit checking system was in China in 1997. Bank staff failed to do an adequate check on this applicant and to check the authenticity of the personal information provided. As we learnt from the interviews, the personal credit checking system is still facing problems caused by the combination of having a big population and limited records. In the big cities, like Beijing, Shanghai and Xi'an, personal credit checking systems have been established recently and have started to provide a reference service for the financial organizations.

Case 2 (Wang 2004, p90):
24th, February 1999, a credit card centre was alerted in a couple of hours by a suspicious transaction amounting to 40,000 RMB (about £4,000) in Hotel A. The following day, three more transactions, each amounting to 18,720 RMB (about £1,872)

were made in the same hotel. The local bank branch contacted the hotel manager and cashiers immediately. Within couple of hours, two suspects were arrested when they were trying to make a purchase at a local shopping mall using a cloned credit card.

This case showed that the cashiers and merchants were lacking in experience when dealing with credit card transactions, but the financial organizations and the police cooperated quickly to combat the fraud.

Case 3 (Wang 2004, p90):
On 8th July 2002, a credit card centre found some suspicious transactions during a routine system check. Following further investigation, the credit card centre focused on 54 customers who applied for credit cards in April, May and June. The total expense involved in was 986,430 RMB (about £98,643). Those transactions were made in two stores in the same shopping mall. One was a fashion and accessories store and the other was an electronic goods retailer. The local branch suspended all these credit cards immediately and reported the incidents to the local Police station. Within two months, five suspects were arrested.

The case displayed collusion between criminals and malicious merchants / agencies. First, criminals bought individuals' personal details from a local car dealer. Those personal details were used to apply for credit cards. The criminals then found a like-minded merchant to process the transactions and to share the monetary value with them.

These cases illustrate weaknesses in the credit card system. The first concerns the use of fake identity in order to obtain a credit card, the second illustrates how card cloning can allow fraudulent transactions to be made over a limited period of time, and the third shows how collusion between customers and merchants can allow fraudulent transactions to be made. In all cases, detection occurred fairly quickly. One problem that the system in China does circumvent is 'card-not-present' fraud, because of the requirement for payment to be made through internet banking channels rather than over the phone.

7.3 Online banking service in China

7.3.1 Overview of online banking in China

The Security First National Bank, launched in America in 1995, was the first virtual bank (Zeng 2006) that was set up specifically to provide financial services through the internet. Other virtual banking operations, like Egg, First Direct soon followed. Many major traditional banks such as HSBC, Barclays and RBS also offer online services in addition to their branch banking activities.

Online banking / financial services in China started in early 1997 (Guo 2004, p17) on a small scale as several industry leaders experimented with building up online payment systems. There are two characteristics of online banking / financial services in China (Lei 2002, p22) worth noting: firstly, there is no purely virtual bank in China so far. All online service providers are traditional banks including the big four state owned banks and several commercial banks. Those banks provide services through both local branches and the internet.

Secondly, there was no protracted development period for online banking / financial services in China. Chinese banks realized the benefits of low cost and 24/7 real time service offered by online banking over other retail channels and over a fairly short time period adopted the models and procedures operating internationally. The following two diagrams (Zhang 2007, p37) show the low cost of financial services provided through the internet in comparison to other service channels for both the USA and China.

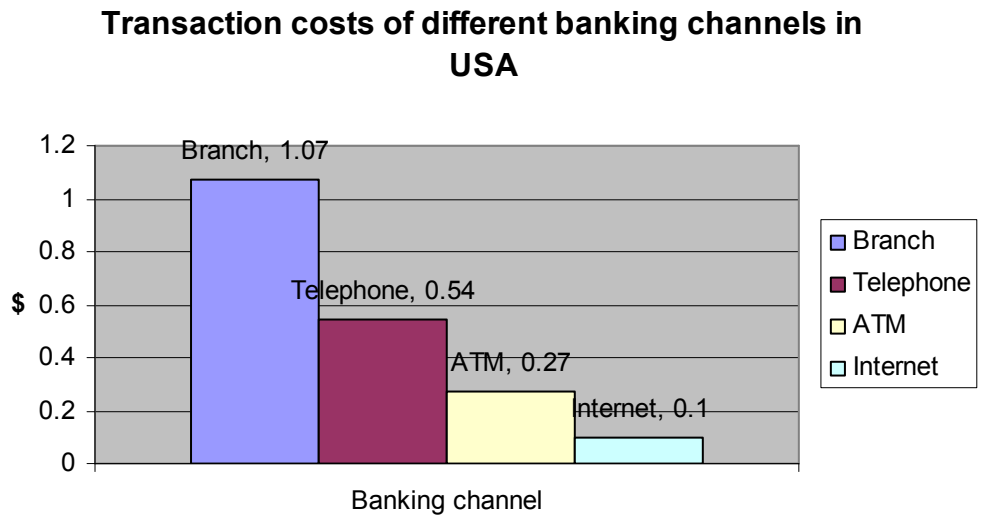


Figure 7.1 Transaction costs of different banking channels in USA

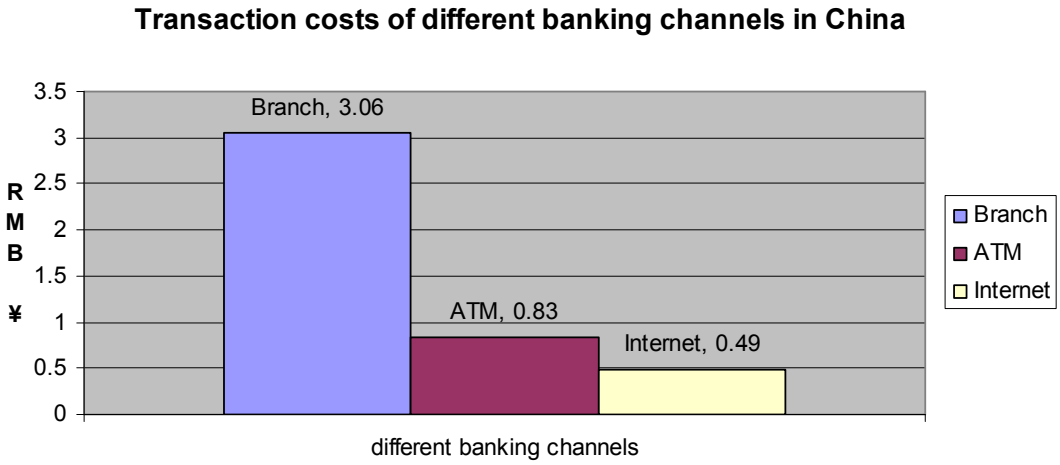


Figure 7.2 Transaction costs of different banking channels in China

Online banking / financial services in China (Lei 2002, p21; Zhang 2007, p37) have been through the following phases of development:

(1) From 1996 to 2000, most banks in China were investing heavily to build up home websites as a new channel for brand promotion, image improvement and information delivery.

(2) From 2000 to 2005 was the initial marketing period for online banking / financial services in China. Banks started to promote basic online functions to individuals (B to

C) and business customers (B to B). Attracted by the low cost of online services, banks were competing with each other to recruit customers. In 2002 (Lei 2002, p21), there were 50 banks providing basic online services in China.

(3) From 2005 till today, a booming period started in China for online banking / financial services, which have shifted from basic functions to advanced services for both individuals and business customers, such as foreign currencies exchange, stock trading and personal investment.

The prosperous development of the internet in China has resulted in China moving ahead of America in 2007 (XinHua News) in terms of having the largest number of internet users in the world. There were over 120 million internet users in China in 2006 (CFCA), 19.4% of whom were also online banking users in 2005 and 33.6% in 2006 (Wang 2007). According to the survey conducted by CFCA (Wang 2007), China Financial Certificate Authority in 2005, online banking users in China have some characteristics in common, for example, a significant number were well educated young professionals aged around 30 years old.

7.3.2 Differences of online banking in China

Compared to western countries, online banking in China is not only a new service channel for customers to manage personal finances but also, or more importantly, it is the critical precondition for shopping online in China. Interestingly, when someone comes to the stage of online payment in China, he or she will be asked to choose a credit / debit card and will be diverted to the website of the online banking service of the relevant bank. Then online shoppers need to log on their online banking accounts and make the payment either using bank cards or making money transfer directly. In brief, if someone wants to make purchase online, he or she must apply for online banking service first in order to make payment online later.

The common way we make online payment in the UK is to submit bank cards details, like card holder's name, card number, expiry date, issue number / security code, postal

address etc to online merchants directly at the merchants' website. Customers in the UK can make a purchase online without using online banking services. Banks are not normally involved in the transaction, although this is changing and with certain credit cards the purchaser is directed to the card-issuer's site and required to provide a 'secure' code for the transaction to proceed (examples of this service include 'NatWest Secure', 'Sainsburys Secure' and 'MBNA Secure').

Online shopping in China seems a little complicated because of the involvement of online banking at the start of the transaction. But that process does increase the security level for online users. Further solutions to secure online transactions in China are various depending on different financial organizations. The top three solutions are One-time PIN generator, Instant Text Message confirmation service and virtual keyboard as we learnt from the interviews with people who work inside financial industry in China.

(1) One-time PIN generator

A one-time PIN generator looks exactly like a mini U drive we use for data storage. Customers will get this small piece of equipment when their applications to online banking service are successful. Different from U drive, there is small screen embedded in the one-time PIN generator showing six-digit code which is used to identify online customers. More interesting, that six-digit code keeps changing every 60 seconds which means that code customers typing to log on personal account online would be different every time. Except for username, password in general use for online banking service, one-time PIN works as an extra security check to protect customers.

The one-time PIN generator is very small with long lasting battery and easy to be carried around, like to attach it on the key ring. With the promotions organized by different banks, customers usually get the one-time PIN generator as a complimentary gift when they apply for the online banking / financial service.

(2) Instant Text Message confirmation service

Even bigger than the population of internet users, by the end of 2008 (XinHua News), the mobile users in China were 64 million of which about 18%, (ie 11.7 million) are accessing the internet using mobile networks. The leading mobile service providers in China (NetEase) estimate that the mobile phone will replace the computer as the primary means of internet access within 3 years in China.

Not surprisingly, more and more banks have started to integrate mobile phone use with the provision of personal financial services. On 1st June 2006 (Guo 2008), the China Construction Bank, one of the big four state owned banks in China, launched an instant financial message service for all customers including account alert, service reminder, transaction confirmation etc. On 12th November 2006 (Guo 2008), the leading mobile service provider, China Mobile was the first to start a campaign for instant financial message service.

Through the interviews with people who work in the financial industry in China, we learnt more details about the instant financial message service. For example, customers can pick different functions, such getting an instant message if there is any balance change; or if there is any purchase online / in person; if there is any attempt to log on the online banking account. More specific, customers can set their own limits / standards for the amount of purchase, withdraw, overdraft etc. For instance, someone will get an instant message when any transaction beyond 5000 RMB (about **£**500) has occurred; another person might be more careful and he wants to be informed if there is any transaction beyond 500 RMB (about **£**50). The instant financial message service can be tailored very well to satisfy individuals' requirements.

(3) Virtual keyboard

As virus / Trojans can copy / record characters and numbers when someone tries to log on the online banking account using the computer keyboard to type username / password, a virtual keyboard works as the extra protection for customers. One of the interviewees, a senior manager in a leading bank in China, expected that the virtual keyboard will replace the traditional computer keyboard for online banking service in the future.

When individuals open the logon web page of an online banking service, a small screen showing a keyboard appears and customers can enter log on information using this virtual keyboard provided by banks instead of the hardware keyboard attached to the computer. More advanced than the fixed hardware keyboard, the settings and orders of the characters and numbers of the virtual keyboard keep changing every time, which means customers don't follow the same typing route every time.

7.3.3 Online banking fraud in China

In comparison to financial organizations, individuals are more vulnerable to fraudulent criminals than companies. There are mainly two types of online banking fraud in China (Yu, Gong 2004) targeting internet users: Phishing attacks and Virus / Trojan attacks:

(1) Phishing attack

Similar to phishing attacks in the UK discussed in chapters 2 and 3, phishing attacks in China also involving sending out millions of emails randomly asking for individuals' banking information. Those malicious emails usually fake as authentic message from leading financial organizations and require sensitive information using the excuses like system update, security alert, and customer service etc. Some of the phishing emails look authentic, even containing links which are used to divert consumers directly to fake websites which look exactly like the authentic websites of financial organizations.

(2) Virus / Trojan attack

Working with a few leading anti-virus software companies in China, Police have arrested groups of suspects who are IT professionals working for criminals to create virus and trojans. These virus and trojans can be embedded into servers, web pages and free downloading documents. When internet users browse a malicious website, virus and trojans will be installed on users' computers automatically. Once individuals' computers have been infected, this malicious software can steal and send

back sensitive information to criminals instantly. They can even record the numbers and characters that individuals type online using the keyboard, capturing for example, usernames, passwords, PIN numbers, account numbers etc.

For internet users who are careless or lack IT skills, vulnerable computers and servers are easily targeted by criminals on the internet. It is essential that individuals who invest in anti-virus software keep it up to date in order to protect the integrity of their systems.

CNCERT / CC (CNCERT), the National Computer Network Emergency Response Technical Team / Coordination Center of China, was founded in 2000 under the supervision of Ministry of Information Industry of China. CNCERT is responsible for public network security nationwide. Also, it cooperates with international police force to against high-tech crimes.

According to the 2007 annual report published by CNCERT on April 2008 (Huanqiu.com), the incidents of website hijacking have been increasing alarmingly from 2003 to 2007 in the China mainland:

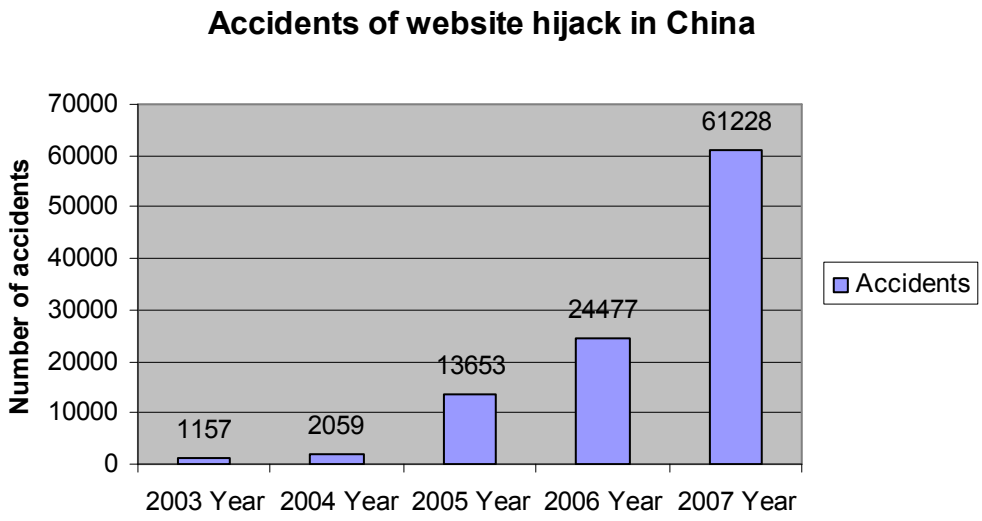


Figure 7.3 Accidents of website hijack in China

In 2007, 61,228 incidents were detected by CNCERT which exposed the vulnerability of websites in China mainland. Among those websites which have been hijacked in

2007, 3407 out of 61,228 targeted local government websites (CNCERT). Some websites even have been attacked repeatedly, causing both financial loss and reputation damage.

The hackers conducting those attacks in China are from different countries worldwide. Among the top ten hackers / hacker groups discovered by CNCERT in 2007 (CNCERT), three are from China mainland while the other seven are organized hackers with strong religious motivations from Turkey.

In 2007 (CNCERT), 1,326 incidents of fake websites were reported to CNCERT worldwide, with 394 complaints being resolved successfully. Most of those attacks targeted the leading financial organizations, such as banks and online payment associations. For example, someone set up a fake website of HSBC using a server located in China to send out millions of phishing emails to bank customers in the UK. It is easy for criminals to commit crime cross border but very hard for any legal authorities to start an investigation overseas efficiently.

With the support from the central government in China (CNCERT), CNCERT established an online community for information collection and security backup in 2005 inviting different organizations from different industries, such as universities, IT companies, retailers etc. Till December 2007(CNCERT), the total 60 organizations have registered and become the members of CNCERT community.

7.3.4 Online banking fraud cases in China

In this section, we paraphrase some cases of fraud involving online banking from examples given in the Chinese banking literature.

Case 1 (Guo 2008, p61):
1st, August 2005 in Yi Zhou, Northern China, Mr. X found out that 23,000 RMB (about £2,300) was stolen from his online banking account. One month later, the suspect was arrested in Guang Zhou, Southern China. The suspect had hijacked

hundreds of bank accounts and stolen 400,000 RMB (about £40,000) in total within seven months.

Case 2 (Guo 2008):

9th, December 2004, a malicious website (www.1cbc.com.cn) which was designed to look like the authentic website of the Industrial and Commercial Bank of China (www.icbc.com.cn) was set up overnight. This bank, which is one of the big four state owned banks in China, is spread throughout the whole country and the false website caused serious damage to the bank both financially and in terms of loss of confidence. On the fake website www.1cbc.com.cn, customers were asked to type in their account number and password. Then an online notice appeared announcing that the system has been suspended due to security reason but would come back to normal in 24 hours. During this period considerable amounts of money were taken out of customers' accounts and extracted from the bank.

Case 3 (Yu, Gong 2004):

May 2005 in Nan Jin, one suspect was arrested by local Police. After further investigation, three more suspects were arrested in two other cities in different provinces in China. These four criminals were in their thirties and had expertise in computer systems and networks. They created and sent out Trojan and virus software on the internet, in particular targeting the servers and websites of financial organizations. At the first attack conducted on 7th, April 2005, they gained account information and passwords illegally within hours after the attack and stole 48000 RMB (about £4800) using online transfer / online banking services.

These cases illustrate some major potential weaknesses in online banking systems, particularly the use of fake websites and Trojan or virus attacks. Clearly customers need to exercise extreme vigilance when making online banking transactions.

7.4 Similarities and Contrasts between the transactions environment in China and the UK.

7.4.1 Fixed interest rate or not

According to the interviews we did in China, the profit that banks or credit card companies in China make from credit card interest amounts to around one third of total profits, whereas in the UK it amounts to approximately half of the profits. The rest of the profits are generated by the merchants' fee, the cardholders' annual fees and other administration fees. In contrast to western countries, in China the APR (annual percentage rate of charge), which varies from credit card to credit card, is fixed by the authority of central government. In other words, all financial organizations in China are carrying the same interest rate of credit card for individuals. The current interest rate on credit cards in China is 0.05%[9] per day, which amounts to around 20% per year on a compound basis.

In contrast to the financial markets in China, financial organizations in the UK enjoy more flexibility about the price and rate of credit card services. The average APR in America is around 10.84% which has been decreased from 14% in the recent two years (52xyk.com.cn). In the UK, credit card offers vary from card type, such as classic, gold, platinum etc, each with a different customer profile. The tables below show the APR borrowing rates offered by financial organizations such as Natwest, HSBC and Barclays.

Table 7.2 Barclays credit cards

(source: (Barclaycard))

Type of credit card	APR (purchase)	APR (cash withdraw)
Platinum	12.4%	27.9%
Flexi-rate	14.9%	27.9%
Classic	19.9%	27.9%
Initial	27.9%	27.9%

[9] http://zhidao.baidu.com/question/42398279.html?fr=ala0 (accessed on 18/05/2010)

Table 7.3 HSBC credit cards

(source: (HSBC))

Type of credit card	APR (purchase)	APR (cash withdraw)
HSBC	16.9-19.9%	23.9-24.7%
Premium	11.9%	11.9%
Student	18.9%	23.6%

Table 7.4 Natwest credit cards

(source: (Natwest))

Type of credit card	APR (purchase)	APR (cash withdraw)
Classic	16.95%	27.95%
Gold	16.95%	27.95%
Platinum	16.95%	27.95%
Student	18.95%	27.95%
Black	13.15%	16.56%
Saving accelerator	16.95%	27.95%
Advantage gold	15.94%	27.95%

Through the tables above, it is easy to find out that the low annual interest rates apply to low risk customers who must reach certain levels of financial standing to be eligible. Banks can use a range of measures to decide on an appropriate credit limit, whereas the APR is a published rate for the type of credit card the individual holds. For individuals who have bad credit history, they would only be eligible to apply for cards with an extremely high interest rate to get credit card services and to repair their credit records. There are several financial organizations that target individuals who have poor credit history. For example, Vanquis Visa Credit Card (Vanquis) claims that they aim to help people who have a history of bad credit, a bad credit rating (including CCJ's—County Court Judgments) and a low income by offering an annual interest rate of 39.94% for purchases and 49.94% for cash withdrawals.

As the interest rates are fixed for the whole credit card market in China, there is no possibility of there being a spectrum of rates aimed at individuals with varying degrees of credit-worthiness. Inevitably, a fixed interest rate reduces the flexibilities of the financial market and the competitiveness of financial organizations in China.

But it helps to keep a relative stable market environment for both financial organizations and individuals in China. Considering the immature financial market and inexperienced consumers, a fixed interest rate works on a positive way to prevent potential risks and vicious competition. This might change in the future as the market becomes more mature.

On the other hand, banks have to take customers seriously to make more profits due to the fixed interest rate in China. Without any possible leverage of prices and rates, banks have to make full use of any opportunity to maintain current customers and to recruit new customers. They offer customers a bewildering choice of tailored financial products and services. At the website of the China Merchants Bank, we found out 12 different categories of credit card, under each of 12 categories, offering different benefits. For instance, one category is designed for female customers only and contains eight different credit card deals combined with membership of shopping malls, fashion magazines, leisure centres etc. As introduced proudly by one of the interviewees, there are more than 100 credit card deals with varied benefits and appearances available for individuals in different age groups, gender, occupations, hobbies and lifestyles. There is professional advice both online and in branches to help individuals to choose suitable credit card deals.

7.4.2 Selection of customers for credit card application

Customer selection, also referred to as customer assessment, is the first priority of risk control of a credit card service – something which was emphasized again and again during the interviews in China. Having observed the development of modern finance in Western countries for decades, Chinese financial organizations have learnt from international competitors and started their own journey carefully. Alerted by the global credit crunch, risk control and customer selection have become the most important strategies for every financial service provider in China.

One key problem, however, is that China did not have a personal credit record system. Challenged by the increase of financial crimes mainly targeting the credit card market

in 2004[10], the central financial administration department in Beijing of the People's Bank of China started to compile a database of personal credit records in a few big cities in China. With the support of all the big four state-owned banks and leading domestic merchants, the personal credit records system has been building up rapidly across the nation since 2005. By the end of 2006[11], it had accumulated personal financial information on 530 million people.

There are three types of the information provided by the personal credit record system in China[12]: (1) Personal identity (e.g. name, ID number, residential address, occupation address etc.). (2) Personal loans / mortgage (e.g. loans / mortgage history, banking details etc.). (3) Credit cards record (e.g. issue banks, credit limit, payment records etc.). After those three main types of information have been established, the system will work on information collection about personal bills, e.g. utility bills, phone bills, income tax, etc. Although personal credit record system has had a good start, it will probably take decades to complete in view of the big population and uneven levels of development across China.

With limited support from the still developing personal credit system, financial organizations have had to adopt extra measures to minimize financial risks associated with individuals. Credit scoring models are still in their infancy in China, and weight tends to be given to individual factors rather than combining them in a comprehensive model. For example, 'age' has become an important factor along with occupation and of course income and asset levels. Interestingly, students' credit card services have been temporarily suspended by all the leading banks because they do not have a stable income. This contrasts to some extent with initiatives in the UK where university students have been targeted by banks, presumably on the basis that students will eventually move into well paid jobs and be good customers in the future.

[10] http://finance.sina.com.cn/money/roll/20061208/11271088472.shtml (accessed on 18/05/2010)
[11] http://finance.sina.com.cn/money/lczx/20061120/05463091395.shtml (accessed on 18/05/2010)
[12] http://finance.sina.com.cn/money/lczx/20061120/05463091395.shtml (accessed on 18/05/2010)

7.4.3 Risk management

For any transactions made by internet banking or bank cards, risks could come from any party involved. All other things being equal, the more parties involved, the more the risks increase. Based on the interviews in China, we found that three strategies about risk control have been adopted by most financial organizations that provide internet banking and bank card services.

(1) Insurance in bulk

Insurance is an efficient and popular way to minimum the risks and losses for any individuals or organizations. As introduced by one of the senior manager who is in charge of one of the credit card centers in China, they opt for insurance to mitigate potential risks and losses caused by individuals. The price banks pay for insurance is much lower than any price in the high street because of the bulk purchase effect, so insurance costs less than one pound per credit card in China per year. According to the discussion with people who work within the financial industry, purchasing insurance is a good solution which benefits both financial organizations and insurance companies. It helps to control the banks' potential liabilities while bringing profits to the insurance companies. Of course, as with any insurance contract, there are potential problems of adverse selection and moral hazard, and from the point of view of the insurance company, it is necessary that the bank does not lower its vigilance on customers just because it is insured (moral hazard), and that the banks that seek insurance are not those which have specific (undisclosed) risks (adverse selection).

(2) Cost increases

In contrast to the emerging banks that adopt the insurance solution, the big four state-owned banks in China usually set aside an amount of profit (ie a reserve or contingency) just in case unexpected situations arise, such as the losses caused by a financial fraud scheme. This strategy has been confirmed by a senior employee who has been working within the financial industry in China for about 15 years. Considering the rather low fraud rate in China, a reserve is very convenient for keeping any problems quietly within the organization. The high interest rates charged

on credit cards are in effect a default premium, so in the normal course of business it is possible to cover any fraudulent losses and still make decent profits.

From the perspective of financial organizations, any damage to their reputations or brands is usually more serious than the financial losses caused by the fraud. That explains why banks would usually help customers to deal with fraudulent cases and sort out everything confidentially. At the fist glance, the banks are trying to help customers to get justice by dealing with malicious merchants or criminals and by refunding customers. In fact, it could be argued that the financial organizations are trying to help themselves to save their own reputations.

During the process of this study, we found it difficult to get accurate figures on financial fraud both in the UK and China. Although we can hear the stories about credit card fraud and read lots of tips and advice about bank card protection in newspapers, magazines, TV programmes, even booklets from the local banks, there is so little information about how bad the losses and damage caused by financial fraud have been. The information available from the newspapers might be just the tip of the iceberg, because the financial organizations involved would never be willing to share or release such information.

That also explains why we must target individuals instead of the financial organizations for data collection. Generally speaking, people are more willing to share and spread the bad experiences than good ones they have had, such as purchases, accommodation, restaurants etc. As it has been proved by the data collection we have done, the respondents who have experienced financial fraud showed their interests in this study by providing detailed information and good quality replies.

(3) Spread loss to other parties involving in the transaction process

Whether a transaction takes place on the internet or in the physical world, it is very likely to have more than one financial organization involved, for example, payment systems and equipments installed in the shopping area might be managed and operated by different financial service providers. The cooperation among the financial

organizations brings convenience and efficiency to the individuals but it makes any case complicated if problems arise.

In China, the losses usually are split to each related parties involved in any fraudulent transactions. For example, suppose a criminal used a stolen credit card and faked the signature to make a purchase in a shopping mall. When the original card holder who is innocent and has nothing to do with the fraud alerted his bank and reported the stolen credit card, credit card issuing bank, the merchants and the shopping mall and the clearance bank would work together to determine how to share the responsibilities and liabilities. For the merchants or shopping mall, they also have to share part of the loss because their employees who worked at the check out counter didn't recognize the fake signature and authorized the fraudulent transaction.

If the fraudulent transaction had been authorized by a PIN number instead of a signature, it means that the merchants would take very little, even no responsibilities for this fraudulent case. The share of losses among each parties involved would be different depending on the specific cases. In general, the original credit card holder would get a full refund if he / she obeys the credit card policies and is not implicated in the fraud.

In contrast to the western countries, any online purchase in China must be connected with a valid online banking account whether using credit cards, debit cards or money transfers. Many banks are working together with reputable merchants to fight credit card fraud and online banking fraud. Individuals can find a detailed list and links to reputable merchants recommended by banks on the banks' websites. The biggest advantage for individuals to make purchase with those recommended merchants is that there is an unconditional guarantee for product / service quality and transaction security.

7.5 Conclusions

This chapter has provided some detailed insights into the transactions systems and banking environment in China, and the differences with the systems and procedures in the UK. This provides a useful background as we now proceed to discuss the construction and analysis of the survey carried out in China.

Chapter 8 China Data Analysis and Summary

8.1 Introduction

In this chapter, we focus on the credit / debit card and electronic banking / payment services in China, the biggest emerging financial market worldwide. Compared to western countries, which have been developing financial framework for centuries, the financial industry and organizations in China are at the beginning of their evolution. However, unlike some of the Islamic countries, they have adopted the popular financial products used by western consumers, such as credit / debit cards, online banking, personal loans etc despite the fact that some of these products have security problems as discussed in the last chapter. It is therefore of particular interest to see how these products perform in a Chinese context and how they are perceived by those who use them. It is this question that is tackled in this chapter, in which a survey similar to the one conducted in the UK is conducted in China and the results analyzed. A comparison of the results together with a discussion of the difference of customers' behaviour and attitudes to the online financial transactions and internet fraud is then presented in chapter 9.

8.2 Data collection in China

8.2.1 Sample Selection

Confidentiality ('customer protection') laws in China meant that the survey had to be approached somewhat differently to that in the UK. Help was solicited from a local bank in Xi'an, which was where the survey was conducted. Xi'an is a large city located in the central part of China and famous for its education resources and outstanding history (including the famous Terracotta Army). The bank, which wishes not to be named for confidentiality reasons, assisted with the selection of bank customers for the survey, the sample consisting of a random selection of the bank's customers who had experience of using credit / debit cards. The bank undertook the tasks of delivery and collection of the questionnaires, something that was necessary because of the rules on customer confidentiality. 500 questionnaires were sent out and

189 replies were received. Of these, 142 were fully completed, giving a valid response rate of 28.4%.

In addition to the survey questionnaire, to provide context and to corroborate the results of the survey, three face-to-face interviews with senior officials working in the financial industry were conducted in different cities in China: one in Beijing (Bank A), one in Shanghai (Bank B) and one in Xi'an (Bank C). Opinions extracted from the interviews are generally corroborated with the analysis.

8.2.2 Data collection bias

As discussed in section 6.2.2 of chapter 6 (UK data analysis & summary), there are two types of data collection bias might appear in our study: selection bias and response bias. Compared to the national statistical figures in China, we noticed the differences when we look at the data of the respondents' highest qualification and age distribution.

The data showed that 64.8% of respondents had a BSc/ BA/ Prof. Qualification. However, the population in China has a much lower education level than developed countries as indicated in the report about the structure of the population in China (wltzq.gov.cn 2004), which showed that the highest qualification in terms of proportions of the population were: BSc/ BA degree, 5.42%; high A-level equivalent, 12.59%; O-level equivalent, 36.93 and GCSE equivalent, 30.44%.

Also, the age distribution of the respondents of the survey was: 52.11% from 21-30 age group, 37.32% from 31-40 age group, 7.04% from 41-50 age group and 3.52% from 51-60 age group. The population structure of similar age groups in China (PR China 2009) was: 15.93% from 21-30 age group, 16.68% from 31-40 age group, 15.50% from 41-50 age group and 11.98% from 51-60 age group. It suggests that the users / customers of bank card / internet banking in China as a whole are likely to be relatively young.

The two differences we discussed above are acceptable because the purpose of the survey was to target people who had experiences about financial transactions on the internet, either been defrauded or not. Supported by the associations found in later sections, younger / better educated individuals are more likely to access to the internet / use bank cards and online banking services in China.

8.3 Data analysis-summary (N=142)

In this section we select a key variable and then look at its relationship with other variables in the same grouping, these groupings being IT skills, age, gender, highest qualification, education background, and usage of credit cards, usage of debit cards and usage of online activities. For example, in the section below, 'IT skills' is selected as the main variable. After looking at its distribution amongst the respondents, its relationship to age, then gender, being defrauded and highest qualification is investigated.

As an initial step, we show below descriptive statistics of two variables: age and gender.

Table 8.1 Age * gender Crosstabulation (CHINA)

			gender		
			male	female	Total
age	21-30years	Count	29	45	74
		% within age	39.2%	60.8%	100.0%
		% within gender	39.2%	66.2%	52.1%
		% of Total	20.4%	31.7%	52.1%
	31-40years	Count	34	19	53
		% within age	64.2%	35.8%	100.0%
		% within gender	45.9%	27.9%	37.3%
		% of Total	23.9%	13.4%	37.3%
	41-50years	Count	8	2	10
		% within age	80.0%	20.0%	100.0%
		% within gender	10.8%	2.9%	7.0%
		% of Total	5.6%	1.4%	7.0%
	51-60years	Count	3	2	5
		% within age	60.0%	40.0%	100.0%
		% within gender	4.1%	2.9%	3.5%
		% of Total	2.1%	1.4%	3.5%
	Total	Count	74	68	142
		% within age	52.1%	47.9%	100.0%
		% within gender	100.0%	100.0%	100.0%
		% of Total	52.1%	47.9%	100.0%

(1) Score of the general IT skill

According to the report published by CNNIC (CNNIC) on December 2009, the number of internet users in China has increased rapidly from 59.1 million in 2002 to 384 million by 2010. Internet has become an irreplaceable activity for people either for work or leisure in China.

51.4% of respondents scored their general IT skills ‘average’. 22.5% and 9.2% scored ‘good’ and ‘very good’. Only 12.7% admitted that the score of their IT skills was below the ‘average’ including ‘very poor’, ‘poor’ and ‘not good’.

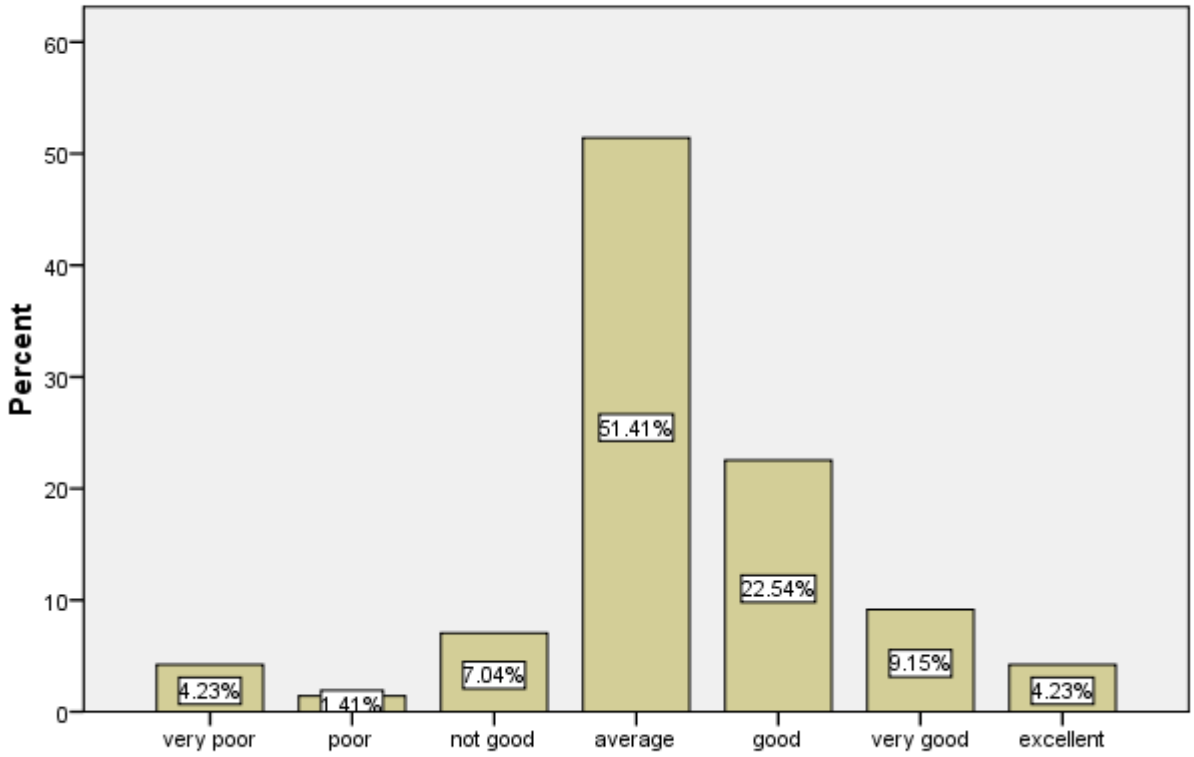


Figure 8.1 Overview of the score of general IT skill

(1.1) Score of the general IT skills and different age groups

We split the variable 'general IT skills' into the different age groups, which have been categorized in the survey question as: <20 year; 21-30 years; 31-40 years; 41-50 years; 51-60 years; 61-70 years and >71 years. The result is shown in Figure 8.2, in which the responses in each group are shown as a percentage of the total number of respondents (rather than as a percentage of the total in each age group) to show in addition how the numbers vary across each age group.

As with the UK, the responses indicate that the older respondents are less confident with their IT skills. Chi-square analysis supported the hypothesis that the older people in China are more likely to have less IT skills because the correlation value is negative (-0.316) and significant (0.001).

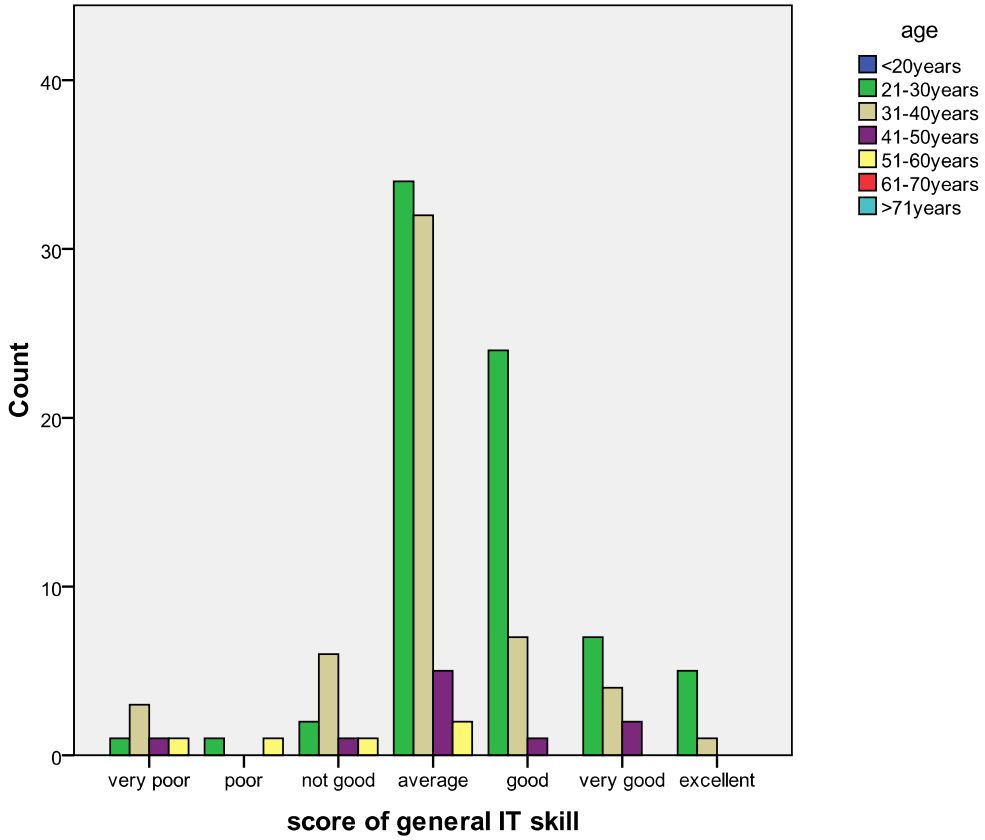


Figure 8.2 Age vs. scores of IT skills

Table 8.2 Cross table of age and score of general IT skill

			score of general IT skill							
			very poor	poor	not good	average	good	very good	excellent	Total
age	21-30years	Count	1	1	2	34	24	7	5	74
		% within age	1.4%	1.4%	2.7%	45.9%	32.4%	9.5%	6.8%	100.0%
		% within score of general IT skill	16.7%	50.0%	20.0%	46.6%	75.0%	53.8%	83.3%	52.1%
	31-40years	Count	3	0	6	32	7	4	1	53
		% within age	5.7%	.0%	11.3%	60.4%	13.2%	7.5%	1.9%	100.0%
		% within score of general IT skill	50.0%	.0%	60.0%	43.8%	21.9%	30.8%	16.7%	37.3%
	41-50years	Count	1	0	1	5	1	2	0	10
		% within age	10.0%	.0%	10.0%	50.0%	10.0%	20.0%	.0%	100.0%
		% within score of general IT skill	16.7%	.0%	10.0%	6.8%	3.1%	15.4%	.0%	7.0%
	51-60years	Count	1	1	1	2	0	0	0	5
		% within age	20.0%	20.0%	20.0%	40.0%	.0%	.0%	.0%	100.0%
		% within score of general IT skill	16.7%	50.0%	10.0%	2.7%	.0%	.0%	.0%	3.5%
	Total	Count	6	2	10	73	32	13	6	142
		% within age	4.2%	1.4%	7.0%	51.4%	22.5%	9.2%	4.2%	100.0%
		% within score of general IT skill	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

(1.2) Score of the general IT skills and gender groups

Figure 8.3 shows IT skill assessment split by gender. There could be a bias if one gender is more modest about its self assessment than the other, but taking the responses at face value, a chi-square test did not find any significant relationship between gender and general IT skills (sig. value = 0.221 and correlation = -0.094). Probably the best way of assessing these responses is to look at them cumulatively from the right – ie to look at the proportions of each gender that assess their abilities at some threshold level or better. If we take the range average or better, 86.5% of males see themselves as being in this range and 88.2% of females – ie very little difference. If we narrow this to good or better, there is a slightly larger difference, with 48.4% of males putting themselves in this category and 33.3% of females, the reason being that some males see their ability very much at the top end of the scale.

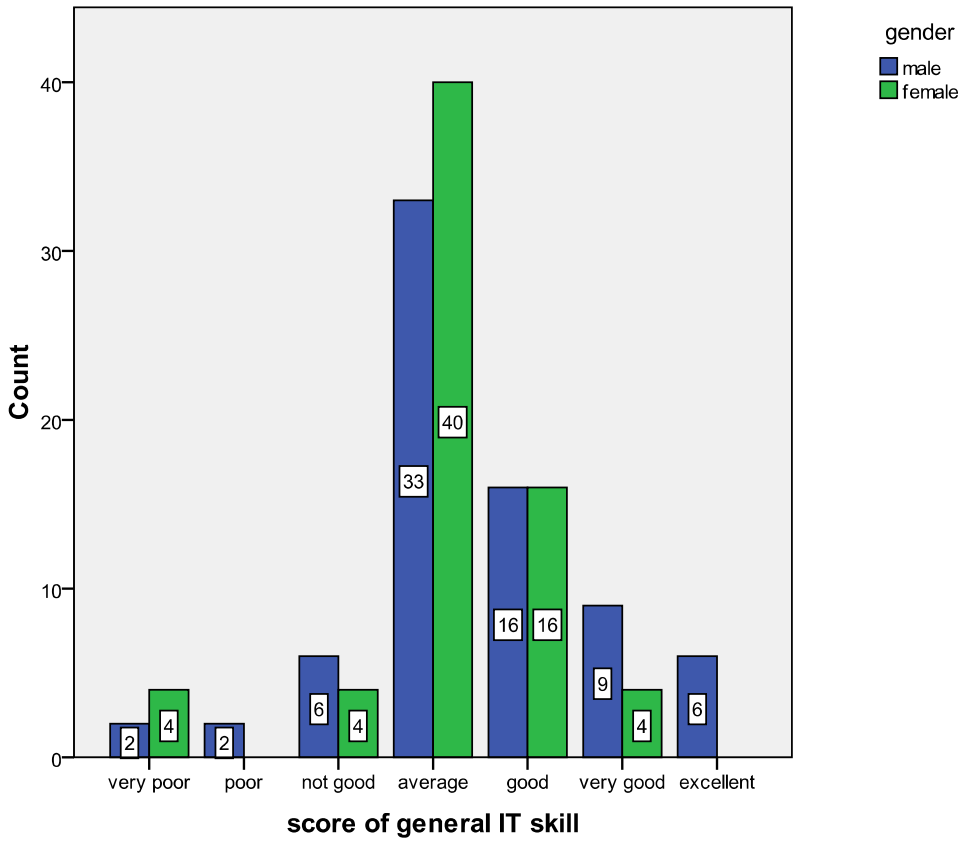


Figure 8.3 Gender vs. score of IT skills

Table 8.3 Crosstable of gender and score of general IT skill

			gender		
			male	female	Total
score of general IT skill	very poor	Count	2	4	6
		% within score of general IT skill	33.3%	66.7%	100.0%
		% within gender	2.7%	5.9%	4.2%
	poor	Count	2	0	2
		% within score of general IT skill	100.0%	.0%	100.0%
		% within gender	2.7%	.0%	1.4%
	not good	Count	6	4	10
		% within score of general IT skill	60.0%	40.0%	100.0%
		% within gender	8.1%	5.9%	7.0%
	average	Count	33	40	73
		% within score of general IT skill	45.2%	54.8%	100.0%
		% within gender	44.6%	58.8%	51.4%
	good	Count	16	16	32
		% within score of general IT skill	50.0%	50.0%	100.0%
		% within gender	21.6%	23.5%	22.5%
	very good	Count	9	4	13
		% within score of general IT skill	69.2%	30.8%	100.0%
		% within gender	12.2%	5.9%	9.2%
	excellent	Count	6	0	6
		% within score of general IT skill	100.0%	.0%	100.0%
		% within gender	8.1%	.0%	4.2%
	Total	Count	74	68	142
		% within score of general IT skill	52.1%	47.9%	100.0%

(1.3) Score of general IT skills and fraud occurrence

Most instances of fraud in the sample occurred to the respondents who were confident with their general IT skills. The most prominent green bars in the graph below fell into the categories to describe the general IT skills as ‘average (2 out of 7)’ and ‘good (4 out of 7)’. A Chi-square test did not support this contention, the correlation being 0.076 with a significance value of 0.430, indicating that there is no significant relationship between IT skill and fraud occurrence. The problem is that with so few

cases of fraud in the China sample, the likelihood of getting a significant test result is low as there are so few degrees of freedom.

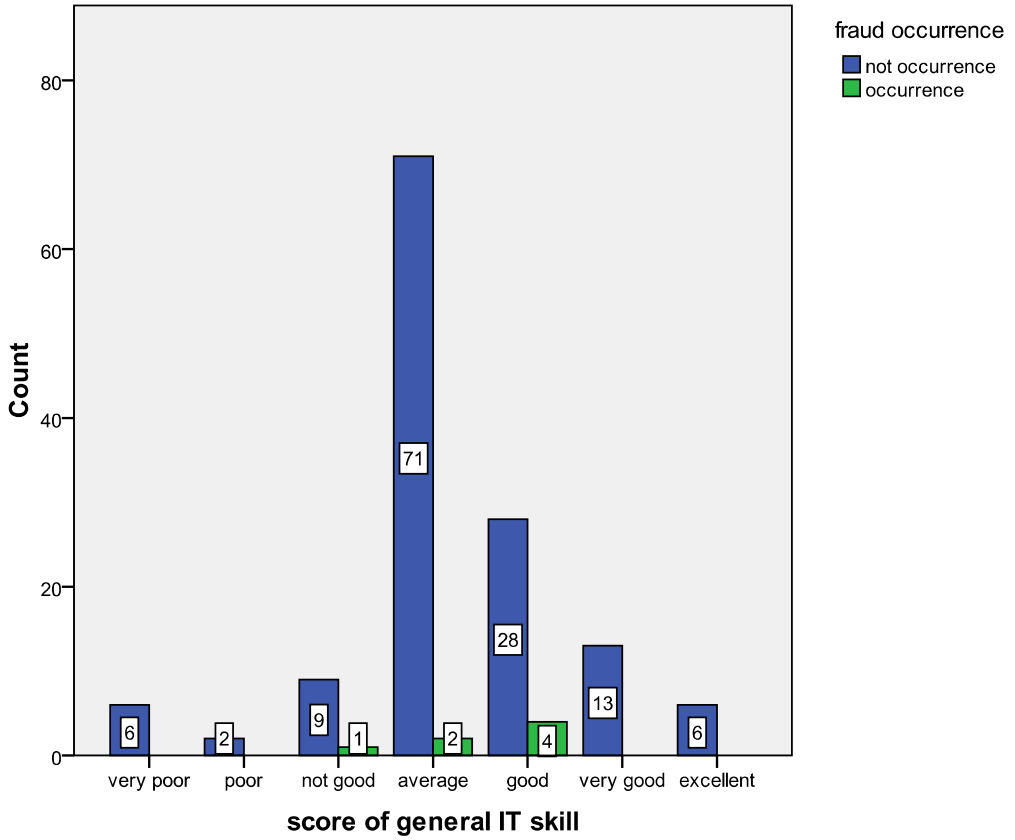


Figure 8.4 Fraud occurrence or not vs. score of IT skills

(1.4) Score of the general IT skills and the highest qualification

When we look at the purple and yellow bars which stand for BSc / BA and further degrees (e.g. MSc / PhD) in the figure below, the top three purple and yellow bars fell into the categories 'average', 'good' and 'very good'. It indicated that respondents who have higher qualification are more confident with their general IT skills.

The Chi-square test gave us the same evidence showing a significant positive relationship between the general IT skill and the highest qualification. The correlation value is 0.210 with a significance value of 0.017, suggesting that people who have higher qualifications are more confident with their general IT skills in China.

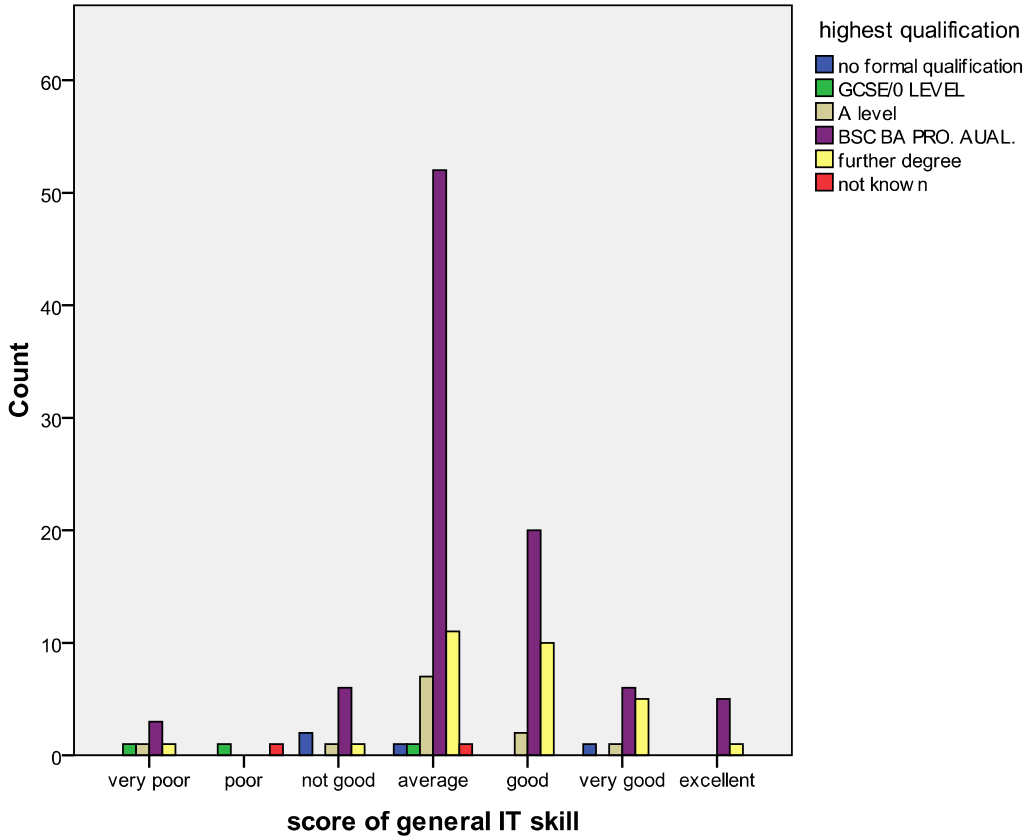


Figure 8.5 Highest qualifications vs. score of IT skills

(2) Age

Because of sensitivity to personal information, we set seven ranges of age for respondents to tick. For the age group <20 years and >71 years, they are less financially active than other 5 groups aged from 21 to 70 years. The following figure showed the age distribution of the survey data collected in China.

In contrast to the age range in the UK data, no respondent in the China survey was aged over 60 years old. 74 (52.1%) respondents were younger than 31 years old. 53 (37.3%) fell into the age group 31-40 years old. Only 10 respondents were from the 41-50 year age group and the remaining 5 respondents were from the 51-60 year age group.

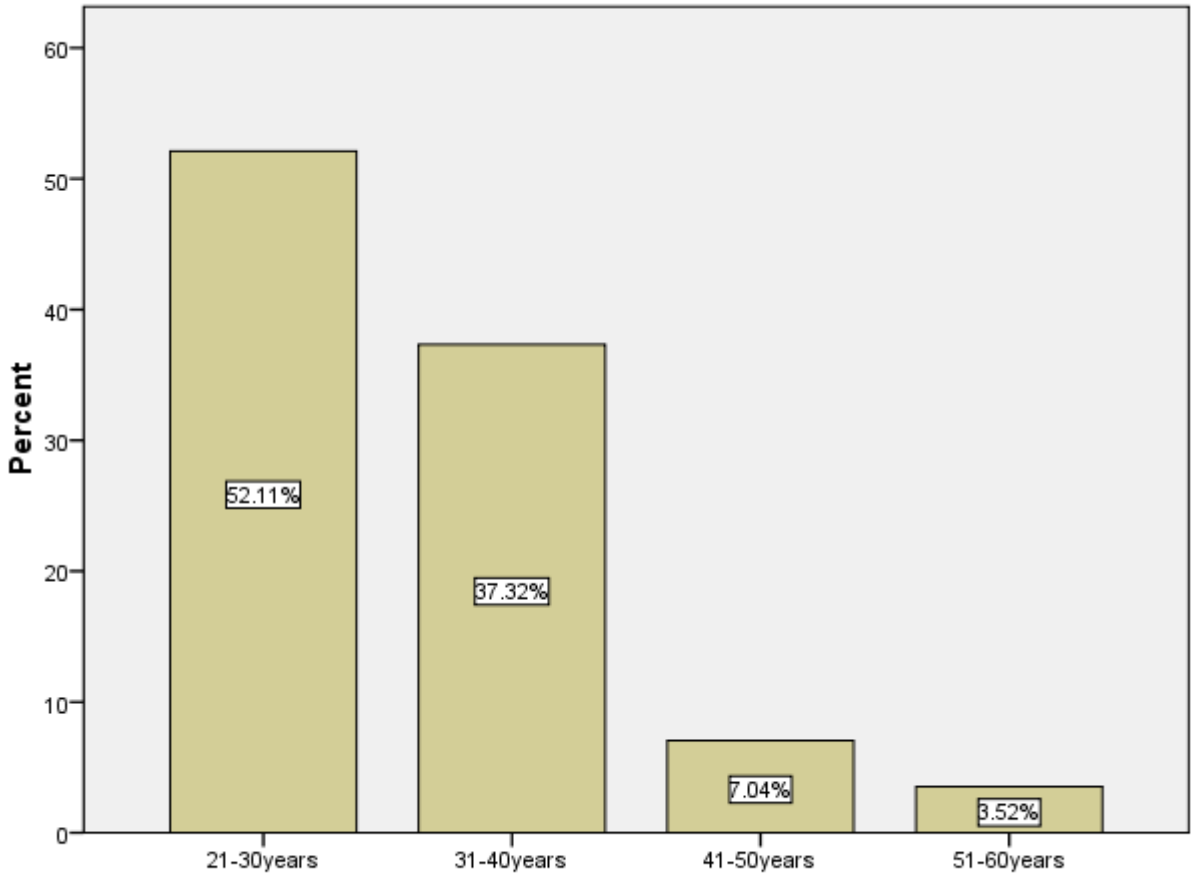


Figure 8.6 Overview of age

The figure suggests that the majority of the users of online financial transactions in China are young (21-30 years) and early middle-aged (31-40 years) individuals. As we would discuss in next chapter, the customers groups of modern finance products in China are college / university students, young and senior professionals. The age group 21-30 years covers the students who are attending higher education and young professionals who have just started their careers after graduation. The individuals from the other group aged 31-40 years are experienced professionals with higher incomes than the 21-30 year group.

(2.1) Age and fraud occurrence

The figure below shows that fraud occurrence (green bars) is spread across different age groups. For the 142 valid responses in total, only seven respondents (4.9%) have

experienced actual financial fraud, two being from the '21-30 age group' and the remaining five from the '31-40 age group'.

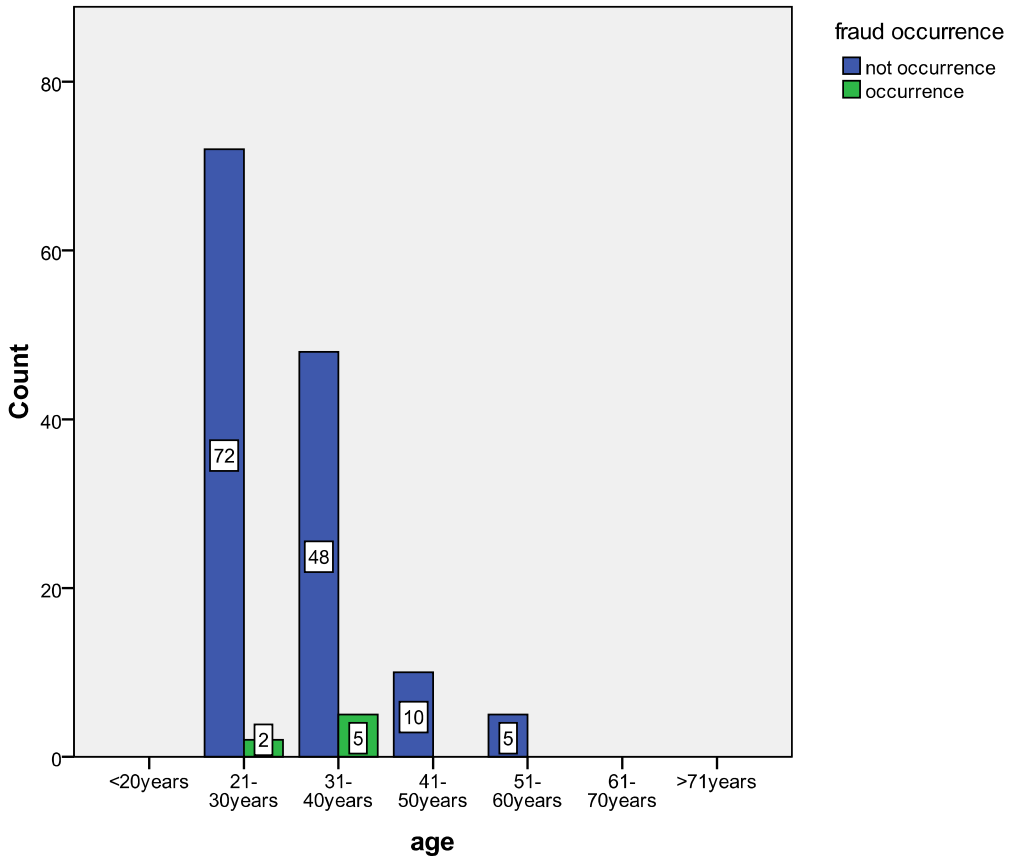


Figure 8.7 Age vs. fraud occurrence or not

However, using a chi-square test we didn't find any significant relationship between age difference and fraud occurrence based on the survey in China (correlation 0.107, sig. value is 0.201), again probably due to the low degrees of freedom in the test.

Looking at the correlation between age and different online activities, we found significantly negative associations appeared between age and online shopping (r = -0.296; Sig. = 0.000); internet banking (r = -0.257; Sig. = 0.002); downloading media (r = -0.174; Sig. = 0.038). The correlation table suggested that younger respondents are more likely to be involved in online activities, as one might expect.

(2.2) Age and Chip-and-PIN usage

The Chip-and-PIN programme has not been introduced to the financial market in China yet, but the use of PIN numbers is widespread and has been for some time. The PIN number works with the card's magnetic strip instead of an embedded chip as in the UK. The difference is not discernible by the cardholder, but the magnetic strip is less secure than a chip and is potentially open to modification by fraudsters. Any transaction made by a debit card requires the input of a six-digit PIN / password to get authorisation (as opposed to four digits with Chip and PIN systems). For credit card payments, normally either a PIN / password or a signature is acceptable – clearly in the latter case the level of security is much lower.

The respondents were not familiar with Chip-and-PIN programme by selecting the 'neither credit nor debit cards' response to the use of Chip and PIN. In contrast, senior professionals within the financial industry in China are well aware of this new approach that was pioneered in France to improve the security level of card transactions. At one of the interviews in China, the interviewee mentioned that the Chip-and-PIN would be launched into China soon and the industry experts are working on a system tailored for the Chinese market.

(2.3) Age and pay off credit card monthly

The following table showed the distribution of whether or not individuals in the survey paid off their credit card balanced each month.

Table 8.4 indicates that younger credit card holders might have a propensity not to pay off their credit card on a monthly basis. Whereas this is consistent with the lifecycle hypothesis, the numbers are too small to draw any general conclusions in this instance. The vast majority of respondents, ie 117 (84.8%), indicated that they would pay off the credit cards every month. 18 respondents (13%) said that sometimes they would pay off monthly and only three respondents (2.2%) said that they would not pay off the credit cards monthly.

Table 8.4 Pay off credit card or not monthly

Age group	Whether pay off credit card or not monthly			
	No	Sometimes	**Yes**	Total
21-30	2	10	**60**	72
31-40	1	7	**44**	52
41-50	0	0	**9**	9
51-60	0	1	**4**	5
Total	3	18	117	138

(3) Gender

The total number of valid responses in the survey conducted in China was 142, of whom 74 (52.1%) respondents were male and 68 (47.9%) are female. The national statistical figure of gender difference in China was 51.5% (male) and 48.5% (female) in 2008 (CPDRC 2008). The difference in proportions between the census data and the survey sample is not significant at the 5% level (based on a binomial test, z = 0.143)

(3.1) Gender and fraud occurrence

The figure below shows that four female and three male respondents experienced actual financial fraud. For the remaining 135 respondents who did not experience actual financial fraud, 71 were male and 64 were female. As expected given these small numbers, a chi-square test did not indicate any statistical significance in the gender difference.

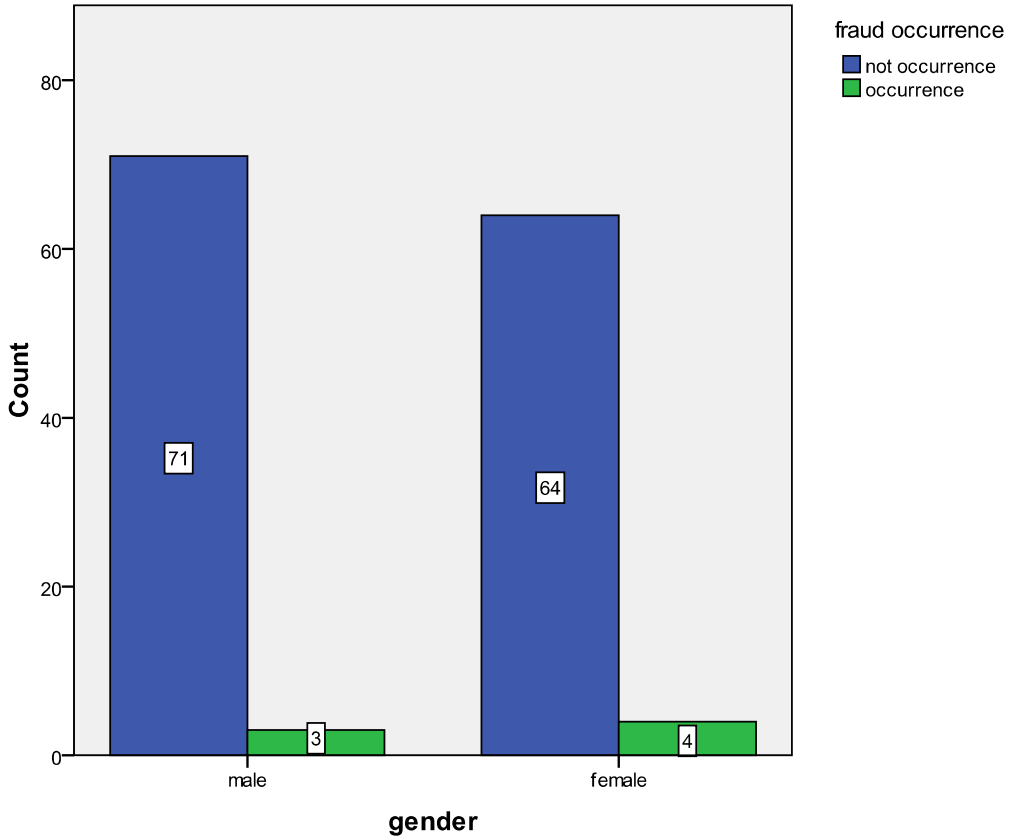


Figure 8.8 Gender vs. fraud occurrence or not

(4) Highest qualification

The respondents were required to describe their highest qualification (if known) using the six categories provided. As previously reported, 92 (64.8%) respondents held BSc/ BA/ Prof. Quali; 29 (20.4%) respondents held further degrees; three (2.1%) respondents held a GCSE/ 0 LEVEL and 12 (8.5%) respondents held an A-level.

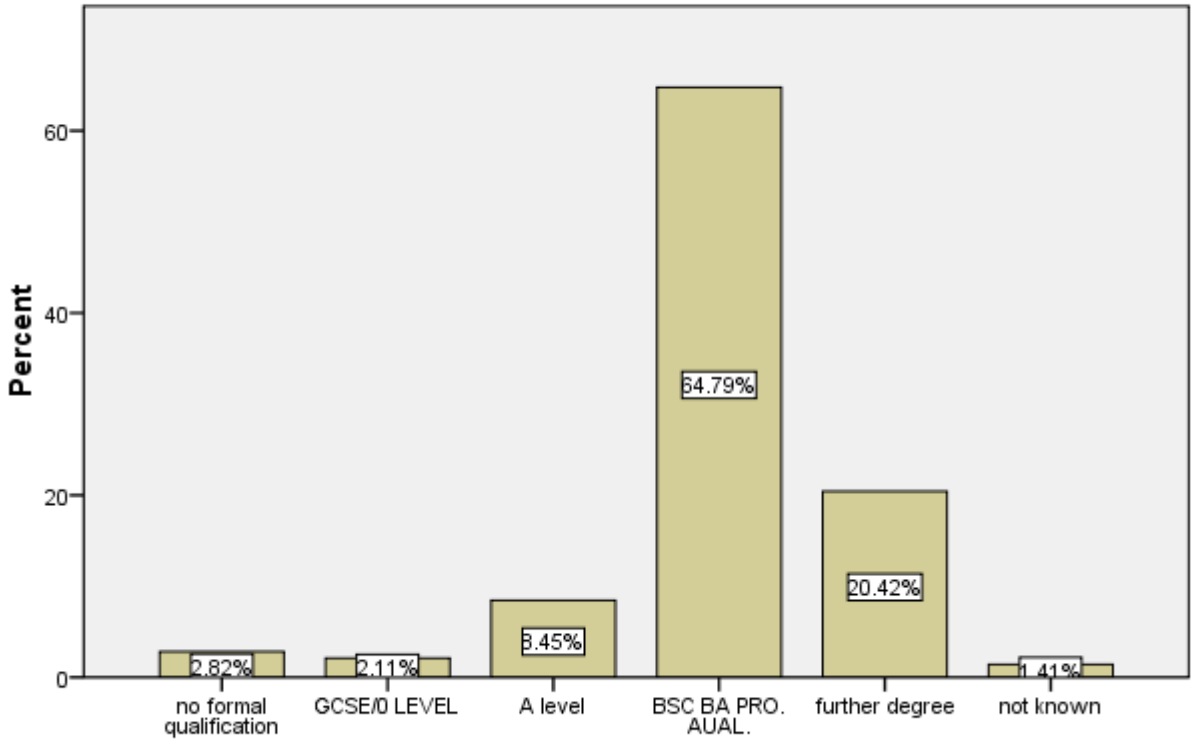


Figure 8.9 Overview of the qualifications of the respondents

(4.1) Highest qualification and fraud occurrence

The table below shows that the seven respondents who were defrauded were well educated, holding a degree like BSc/ BA or higher qualifications.

Table 8.5 Qualification vs. fraud occurrence or not

Qualification	Fraud occurrence	Fraud not occurrence	Fraud rate
No formal qualification	0	4	0
GCSE / 0 level	0	3	0
A level	0	12	0
BSc / BA/ Prof. Quali.	**5**	87	5.4%
Further degree	**2**	27	6.9%
Not known	0	2	0
Total	**7**	135	4.9%

Despite the apparently association between higher level qualifications and suffering fraud indicated in the table, no significant relationship is indicated by a chi-square test.

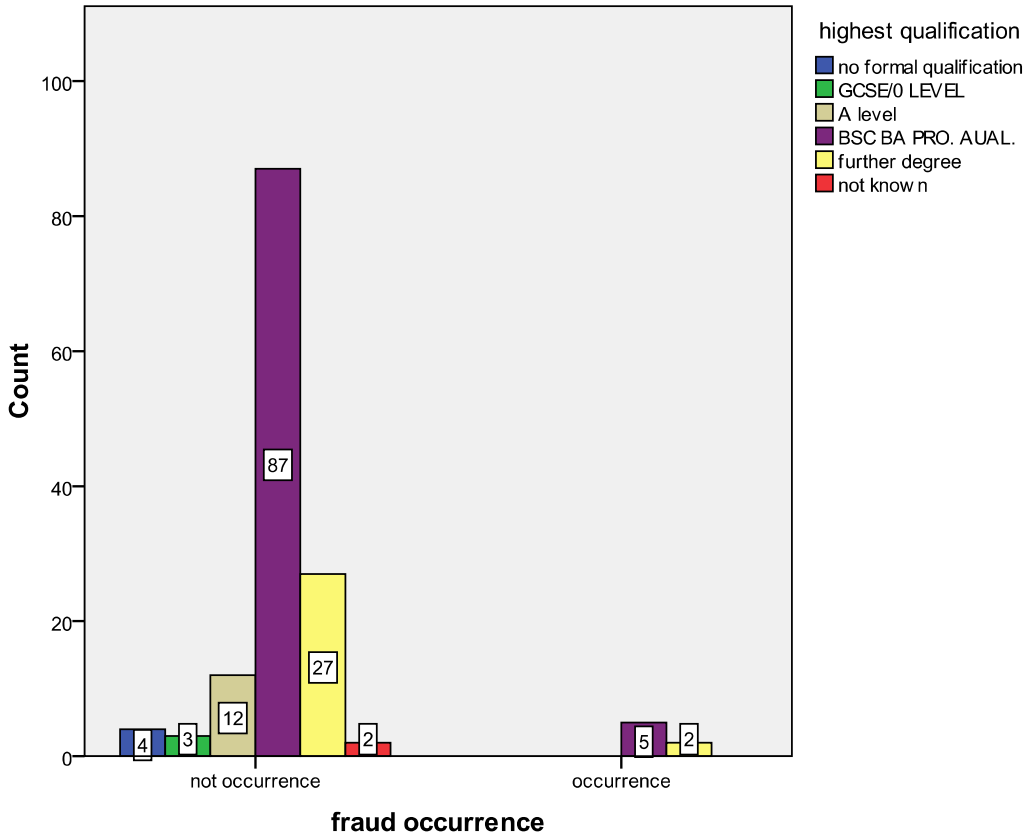


Figure 8.10 Highest qualification vs. fraud occurrence or not

(5) Education background is IT related or finance related

This question was designed for the purpose of investigating whether or not a background in IT or finance would make any difference to the incidence of internet fraud experienced. 142 valid replies were collected: 56 (39.4%) respondents studied neither IT nor Finance; 61 (43%) respondents studied Finance; nine (6.3%) studied IT and 16 (11.3%) had an education background related to both IT and Finance.

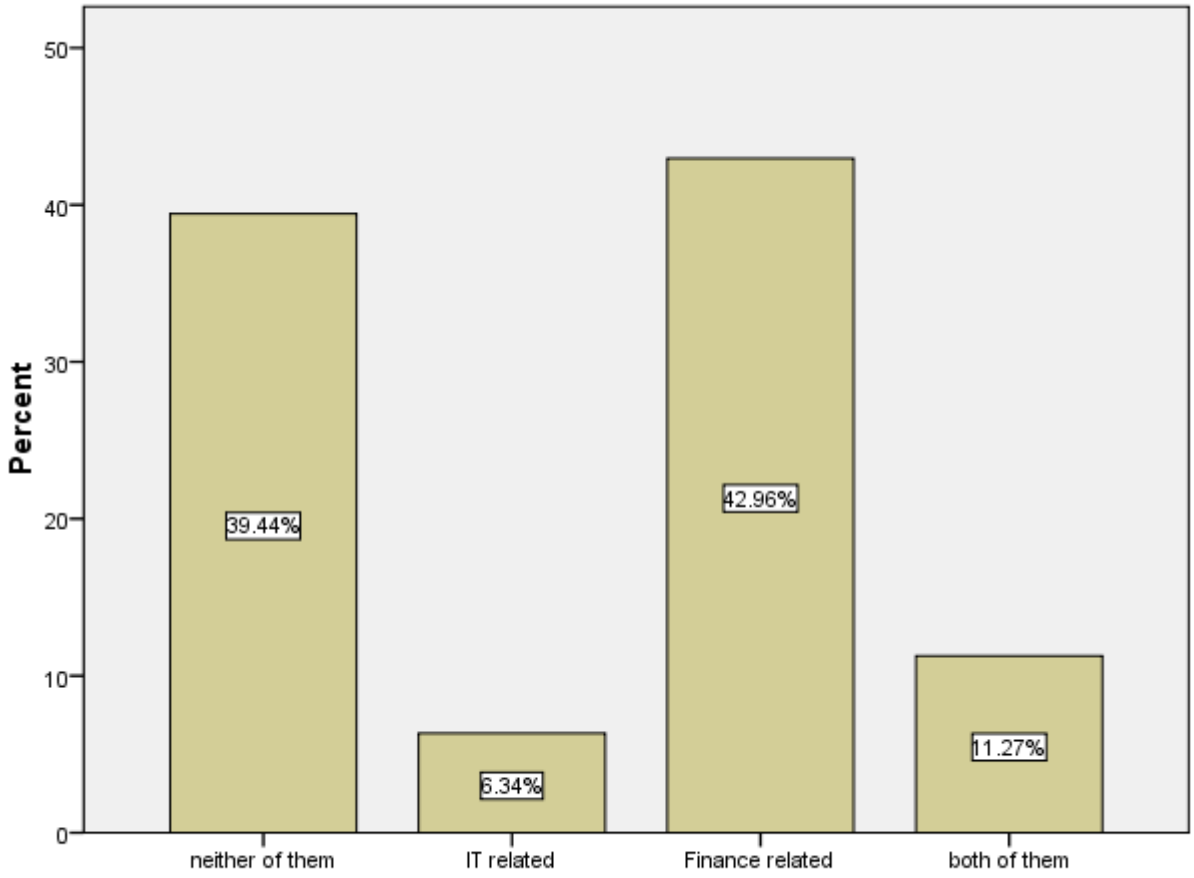


Figure 8.11 Overview of Education background related to IT or finance

(5.1) Education background is IT related / Finance related and fraud occurrence

Of the seven individuals in the China survey who had experienced fraud, five (71.4%) studied finance; one had an education background related to both finance and IT and the other held an education background related to neither finance nor IT. Although not statistically significant because of the small number who had experienced fraud, there is a suggestion that those with a finance background might be more susceptible.

(5.2) Relationship between IT / Finance background and age group

The following diagram shows the relationship between IT / Finance background and age group. Given that both IT and Finance are modern disciplines the diagram shows the expected trend with no-one above the age of 51 having a background in these areas.

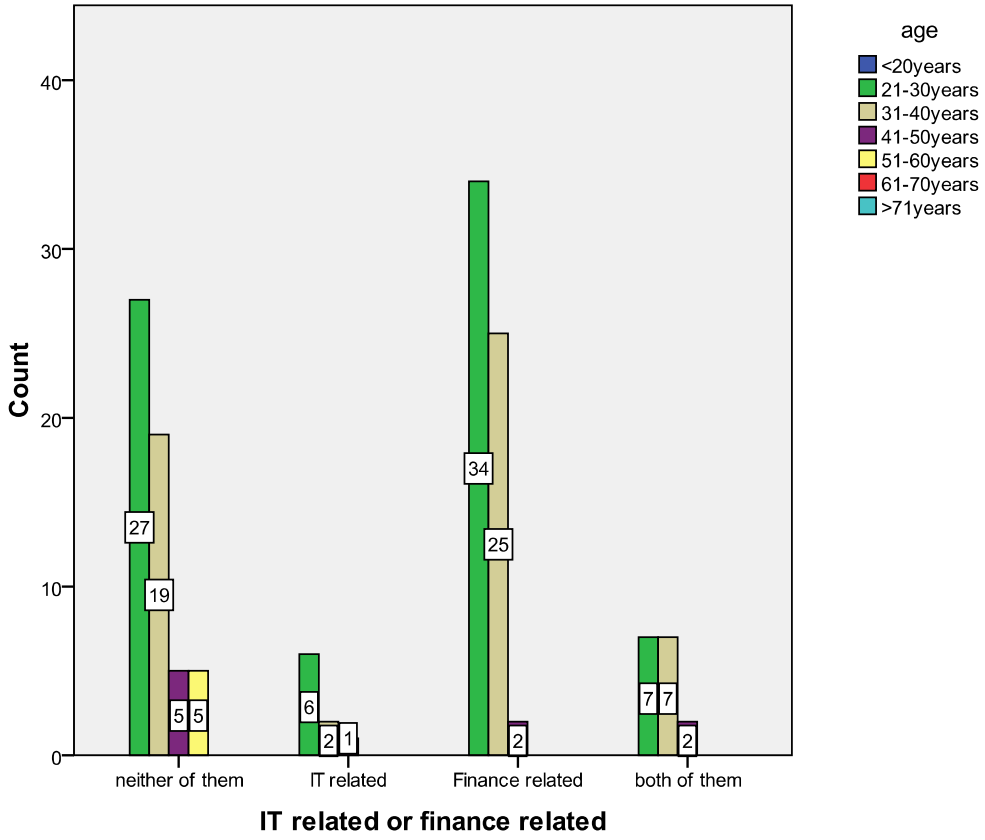


Figure 8.12 Education vs. age

Table 8.6 Cross table of age and education background

			IT related or finance related				
			neither of them	IT related	Finance related	both of them	Total
age	21-30years	Count	27	6	34	7	74
		% within age(3.1)	36.5%	8.1%	45.9%	9.5%	100.0%
		% within IT related or finance related(3.4)	48.2%	66.7%	55.7%	43.8%	52.1%
	31-40years	Count	19	2	25	7	53
		% within age(3.1)	35.8%	3.8%	47.2%	13.2%	100.0%
		% within IT related or finance related(3.4)	33.9%	22.2%	41.0%	43.8%	37.3%
	41-50years	Count	5	1	2	2	10
		% within age(3.1)	50.0%	10.0%	20.0%	20.0%	100.0%
		% within IT related or finance related(3.4)	8.9%	11.1%	3.3%	12.5%	7.0%
	51-60years	Count	5	0	0	0	5
		% within age(3.1)	100.0%	.0%	.0%	.0%	100.0%
		% within IT related or finance related(3.4)	8.9%	.0%	.0%	.0%	3.5%
	Total	Count	56	9	61	16	142
		% within age(3.1)	39.4%	6.3%	43.0%	11.3%	100.0%
		% within IT related or finance related(3.4)	100.0%	100.0%	100.0%	100.0%	100.0%

(6) Usage of credit card

(6.1) Number of credit card

In the survey data, seven (4.9%) the Chinese respondents did not have any credit cards, the smallest number being zero and the highest was the surprisingly large number of 20, the average being 2.68 credit cards per person. In the Chinese economy as a whole, the average number of credit card held is the not dissimilar figure of 2.8[13]. Returning to the survey data, approximately 10% of respondents had five or more credit cards, possibly reflecting the fact that different cards qualify for discounts in different outlets.

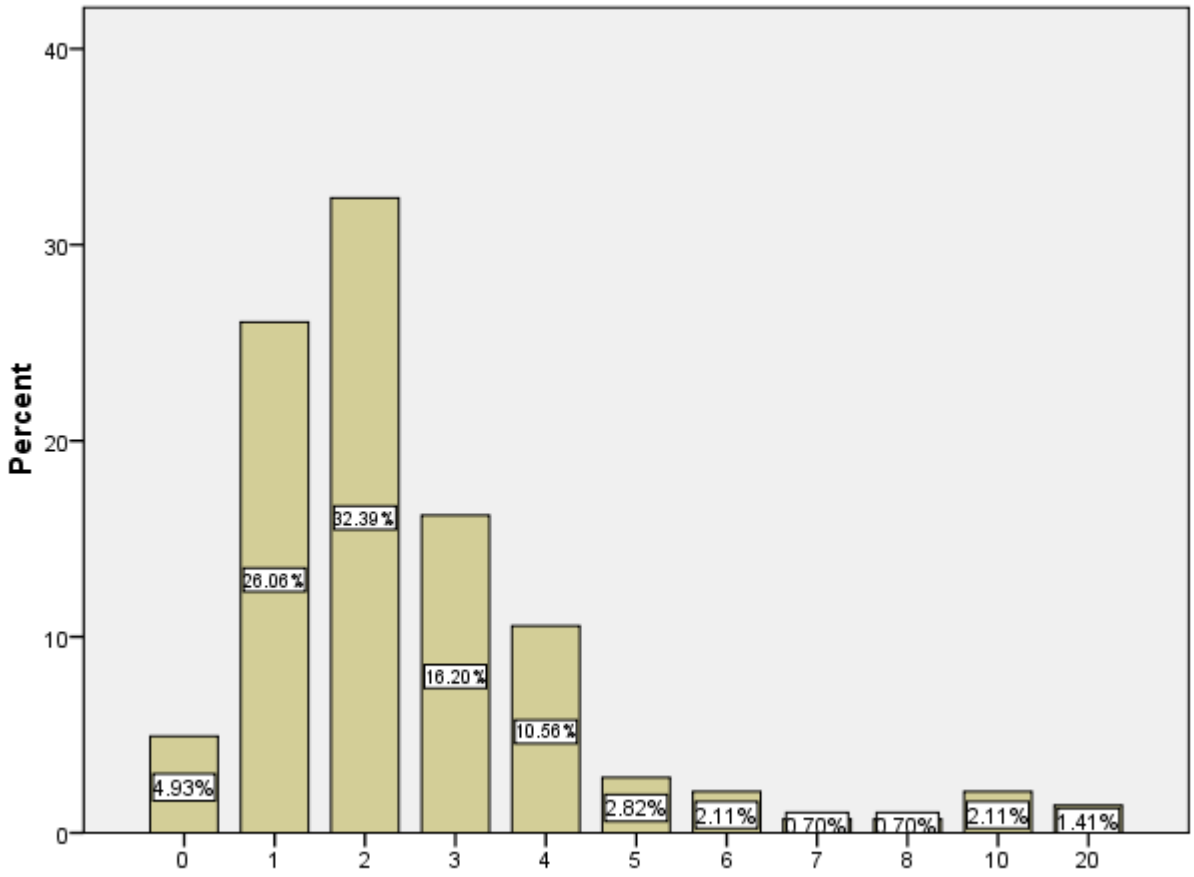


Figure 8.13 Overview of number of credit cards owned

[13] Source from a professional within the financial industry in China in 2009.

(6.2) Number of years of credit card usage

135 out of 142 replies from China provided a figure for the number of years of credit card usage, ranging from one year to 15 years. The average length of credit card usage is 4.13 years, which is much lower than the average derived from the respondents in the UK (19.4 years) mainly because the credit cards usage have been popular for decades in western countries.

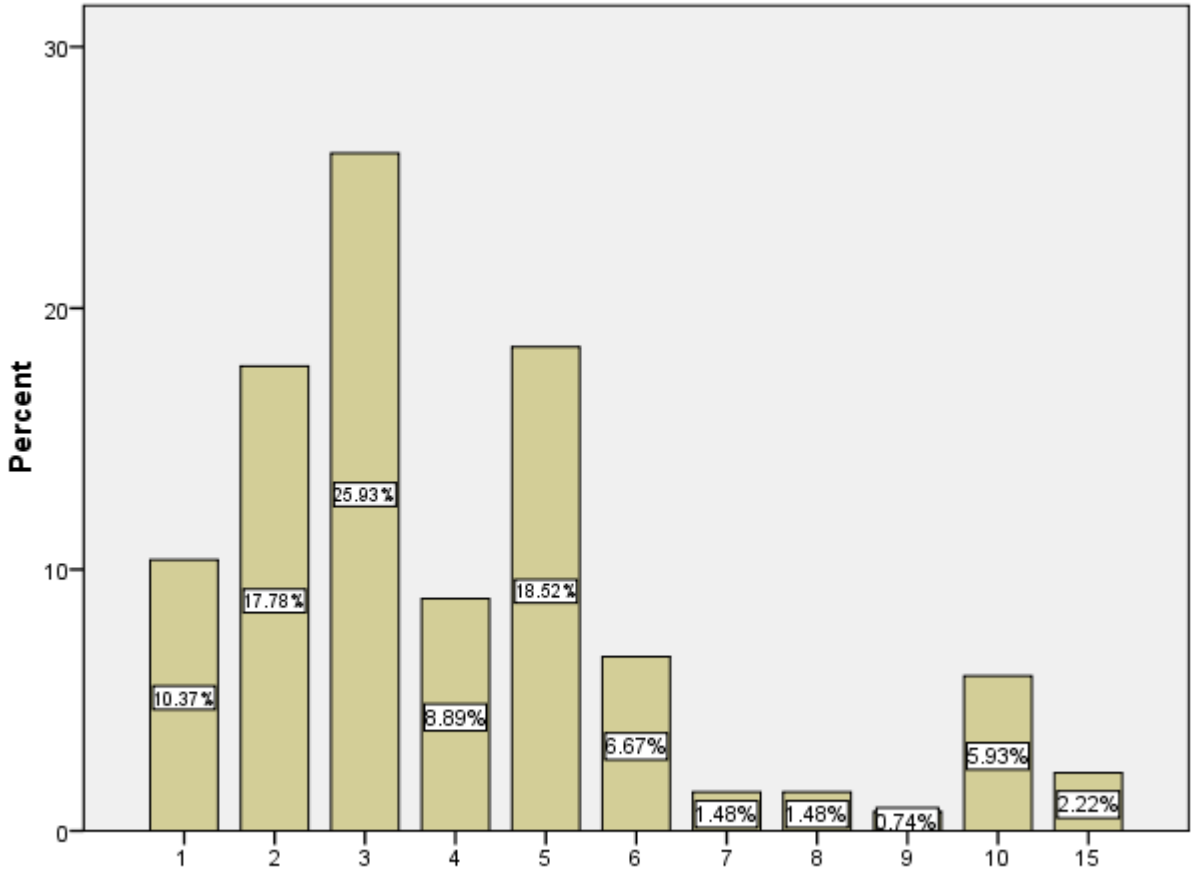


Figure 8.14 Overview of number of years of credit card usage

(6.3) Customers' satisfaction with credit cards

We used five scales (from 1 to 5) in both China and UK to measure the customers' satisfaction with credit card services. 135 out of 142 respondents in China answered this question and the rest 7 respondents left the question blank. Those 135 valid data covered all five scales: not satisfied at all =1; not satisfied =2; average =3; satisfied =4 and very satisfied =5.

117 (86.7%) gave positive responses to the credit card services as the following: 39.3% average; 36.3% satisfied and 11.1% very satisfied. This leaves over 13% who were not satisfied compared to only 3% in the UK survey. A possible explanation as learnt in one of the interviews in China, is that most complaints about credit card services were due to misunderstanding between customers and banks in such areas as interest calculations, the payment period and the service fee charge. As discussed in chapter 3 (section 3.3.4) many of the published 'terms and conditions' are vague about these and other important matters.

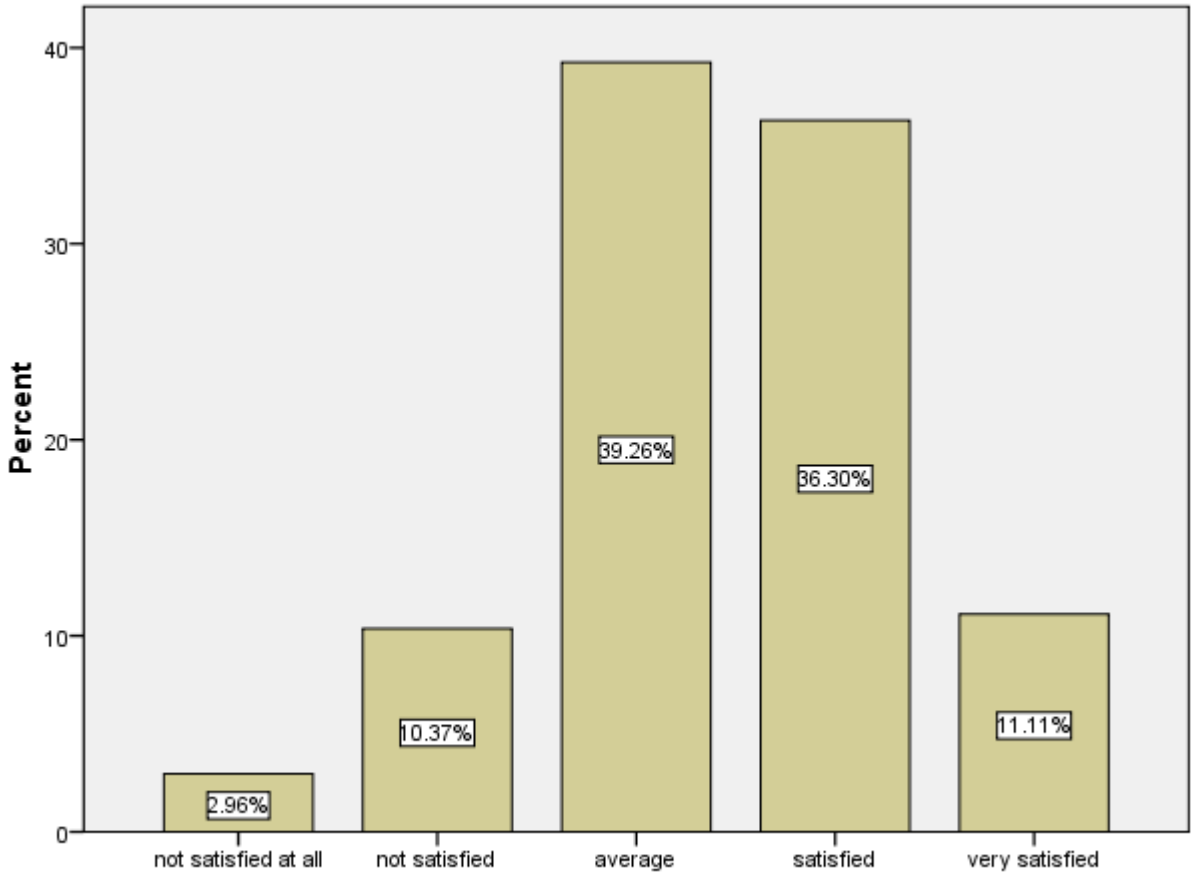


Figure 8.15 Overview of customers' satisfaction with credit card

(6.4) Customers' satisfaction in relation to fraud occurrence

The green bars standing for the fraud appeared into the categories: average, satisfied and very satisfied. An interesting question is whether the satisfaction levels of those who had been defrauded differed from those who had not. Of the seven respondents who had been defrauded, three ticked 'average' to describe their satisfaction level

with the credit card service in China; three were satisfied with the credit card services and only one of these customers indicated that he or she was very satisfied with the credit card service in China. It does not seem therefore as though there is any systematic relation between satisfaction levels and whether or not a respondent had been defrauded, a fact that was supported by a formal chi-square test (sig value = 0.884, r = 0.068).

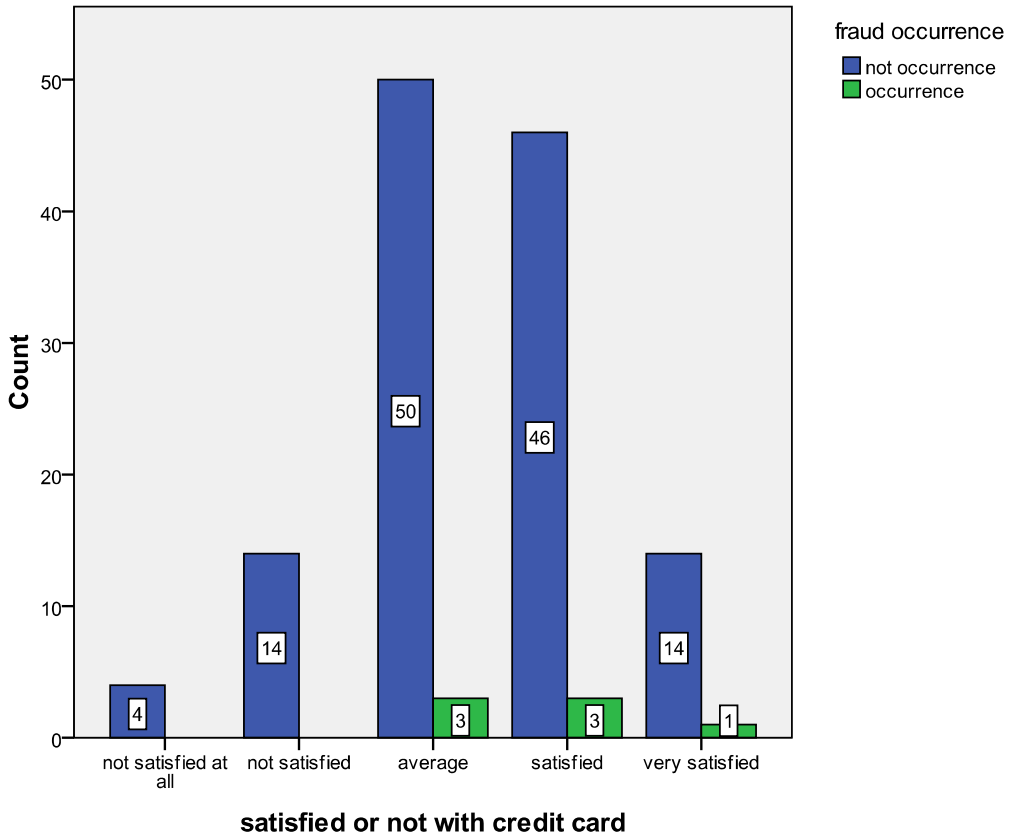


Figure 8.16 Customers' satisfaction with credit card vs. fraud occurrence

(7) Usage of debit cards

(7.1) Number of debit cards

142 of the respondents indicated their possession of debit cards, the lowest number being zero and the highest 10, which is rather more than the highest number for the UK of 6. The average number of debit cards held per person is 3.32 based on the survey data while 2.6[14] is the official number of debit card held per person in China.

[14] Source from a professional within the financial industry in China in 2009.

These averages are again higher than those for the UK, which were 1.63 for the survey sample and an 'official' average of 1.6. The implication is that the respondents to the China survey had more bank accounts, which might be explained by the tendency for people changing jobs to open a new bank account for salary payments by their new employer, rather than to use existing bank accounts.

In comparison to the finding in the previous section that only 7 (4.9%) of the Chinese respondents did not have any credit cards, only one individual (0.7%) did not have any debit cards. In the survey sample, the average number of debit cards held, which was 3.32, exceeded the average number of credit cards, 2.68, suggesting that debit cards are more popular than credit cards in China. This contrasts with the position in the UK, where very few people hold more than two debit cards.

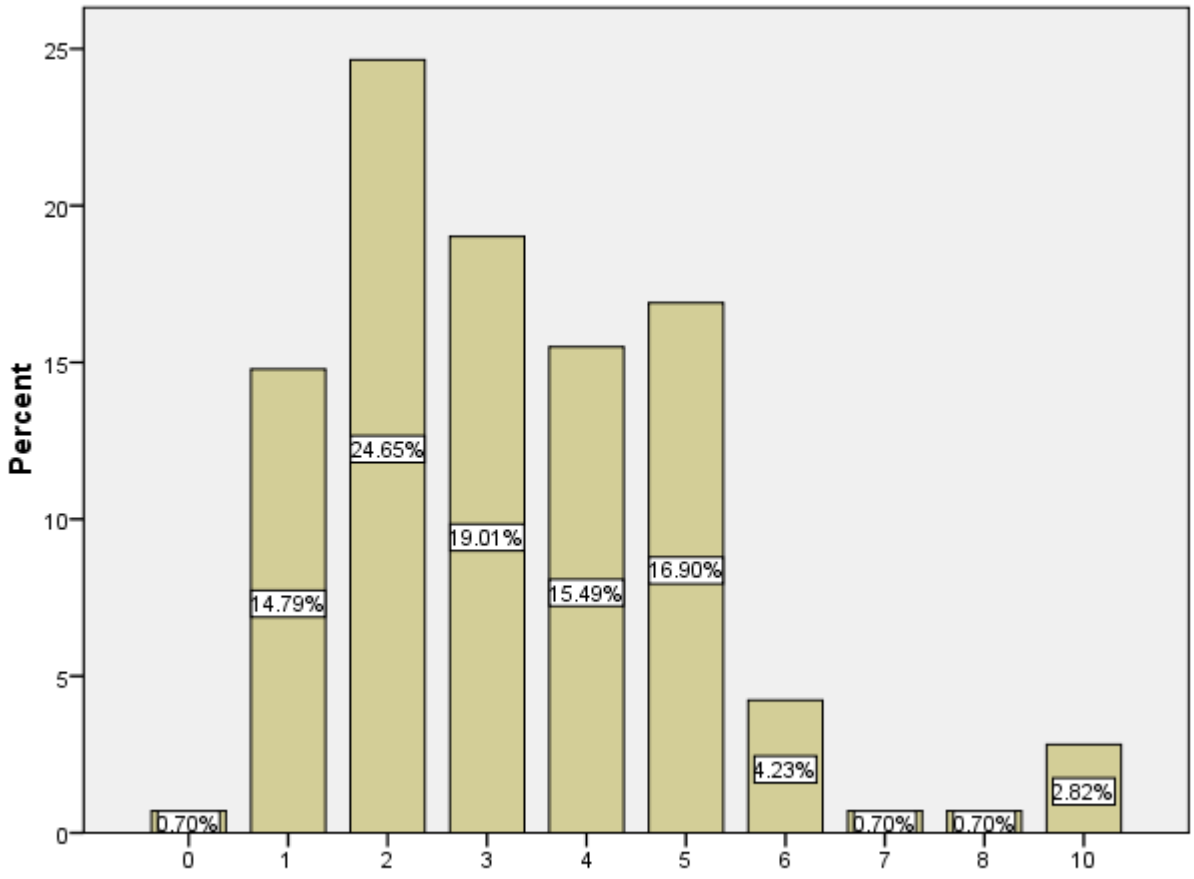


Figure 8.17 Overview of number of debit card owned

(7.2) History of debit card use

141 respondents provided the number of years of debit card usage, the lowest being one year and the highest 30 years. The average length of debit card usage in the China sample is 8.13 years, which is much shorter than in the UK sample where the average length of debit card usage was about 18.1. This partly reflects that fact that debit cards are comparatively new in China, but also is a consequence of the age distribution of the UK sample, where there were relatively more respondents in the higher age categories.

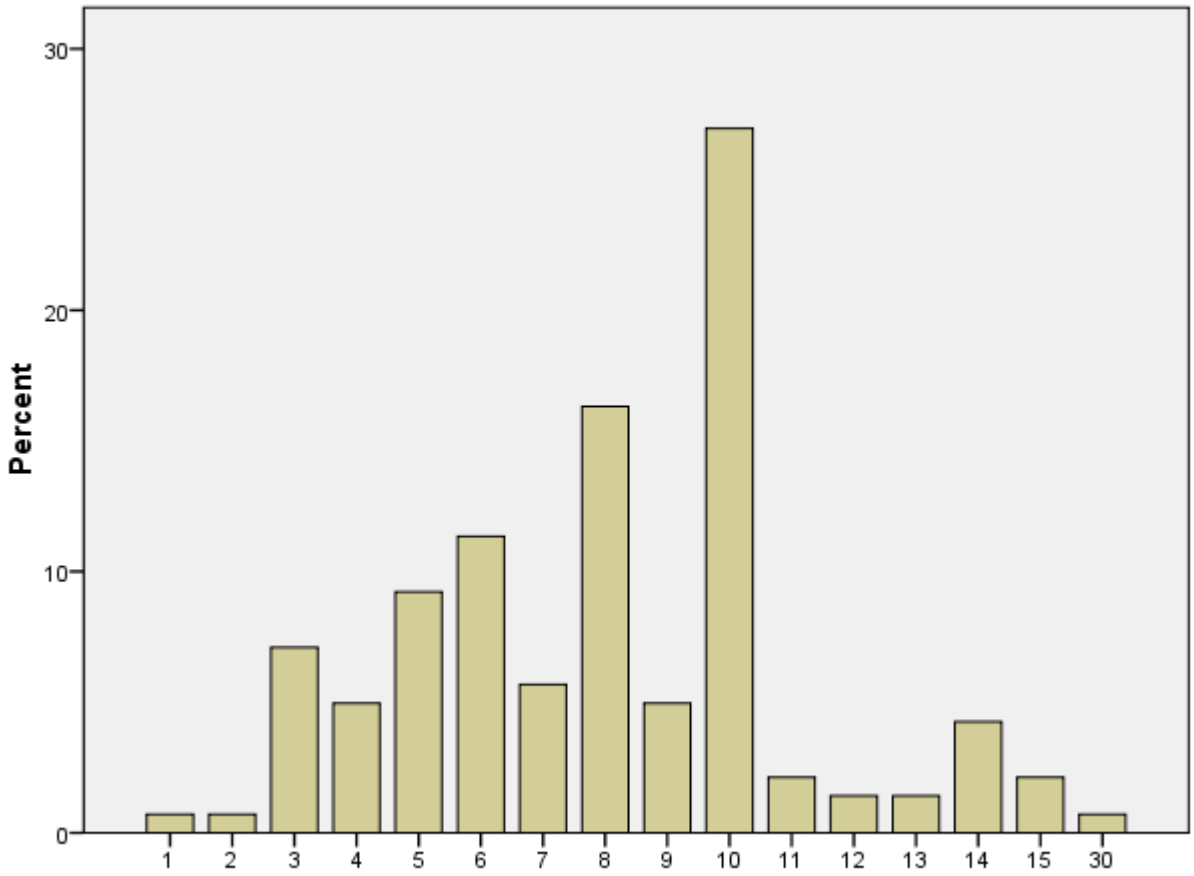


Figure 8.18 Overview of number of years of debit card usage

(7.3) Customers' satisfaction with debit cards

We used five scales (from 1 to 5) to measure the customers' satisfaction with debit card services. 141 respondents in China answered this question and only 1 respondent left the question blank. The 141 valid responses were spread over five scales (not satisfied at all=1; not satisfied=2; average=3; satisfied=4 and very satisfied=5). 130 respondents (92.2%) gave positive responses as follows: 43.3% average; 39.0% satisfied and 9.9% very satisfied. This leaves 7% who were not satisfied compared to about 2% in the UK sample. As reported by 'Morning Shanghai (Netease 2008)' on 04 Oct. 2008, one of the leading newspapers in China, debit cards service is not free any more. Banks started to announce that service charge of debit card usage will be adjusted in the following week in order to encourage individuals' usage of debit cards. Similar comments given by an interviewee in China, banks were trying to make customers to usage debit card more frequently by increasing the service / administration charge, in particular targeting the individuals who only make card transaction occasionally.

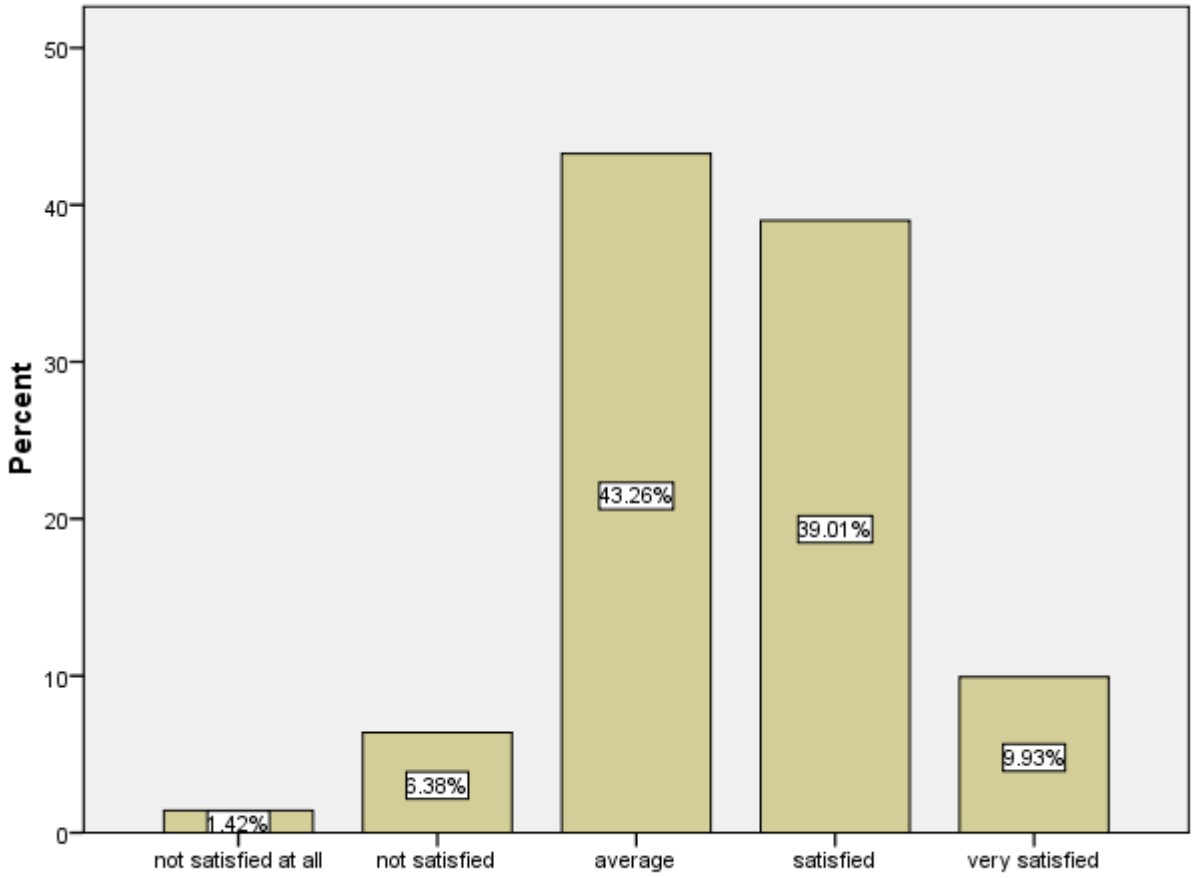


Figure 8.19 Customers' satisfaction with debit card usage

(7.4) Customers' satisfaction with debit cards relative to fraud occurrence

The question of interest is whether those who had been defrauded had similar or altered levels of satisfaction compared to those who had not. In the diagram below, the green bars representing those who had been defrauded appeared were in the three categories: average, satisfied and very satisfied. In other words, individuals who have been defrauded gave out more positive comments about the satisfaction with the debit card service in China than those who had not, suggesting that defrauded customers are generally pleased with how the banks / credit card companies dealt with fraudulent incidents. Again, because of the low number of defrauded customers, the statistical test for association did not register a significant result.

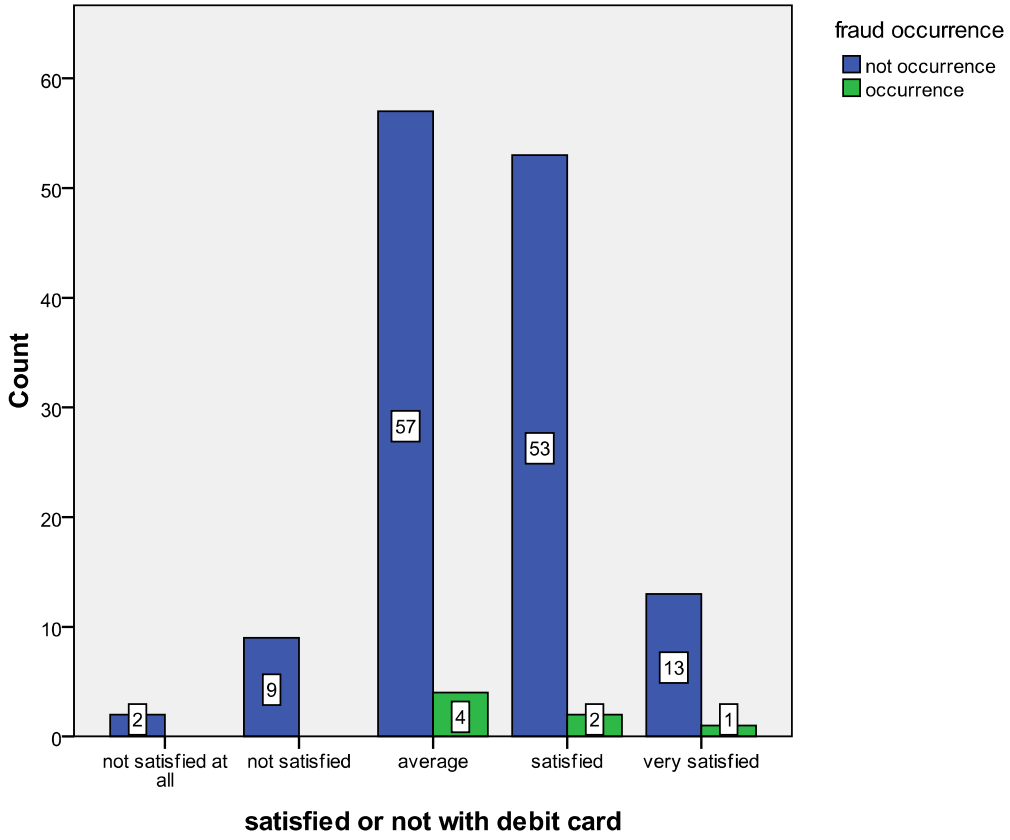


Figure 8.20 Customers' satisfaction with debit card vs. fraud occurrence

Table 8.7 Cross table of customers satisfaction and fraud occurrence

			fraud occurrence		
			not occurrence	occurrence	Total
satisfied or not with debit card	not satisfied at all	Count	2	0	2
		% within satisfied or not with debit card	100.0%	.0%	100.0%
		% within fraud occurrence	1.5%	.0%	1.4%
	not satisfied	Count	9	0	9
		% within satisfied or not with debit card	100.0%	.0%	100.0%
		% within fraud occurrence	6.7%	.0%	6.4%
	average	Count	57	4	61
		% within satisfied or not with debit card	93.4%	6.6%	100.0%
		% within fraud occurrence	42.5%	57.1%	43.3%
	satisfied	Count	53	2	55
		% within satisfied or not with debit card	96.4%	3.6%	100.0%
		% within fraud occurrence	39.6%	28.6%	39.0%
	very satisfied	Count	13	1	14
		% within satisfied or not with debit card	92.9%	7.1%	100.0%
		% within fraud occurrence	9.7%	14.3%	9.9%
	Total	Count	134	7	141
		% within satisfied or not with debit card	95.0%	5.0%	100.0%

(8) Usage of online activities

In this section, the connection between experiencing fraud and use of a range of online activities is explored, to explore the extent to which the use of online services is associated with the propensity to be defrauded.

Table 8.8 Usage of online activities in relation to fraud occurrence

Online activities	Usage of online activities		Correlation with being defrauded	Sig.
	Yes	No		
Internet banking	98 (69%)	44 (31%)	-0.058	0.490
Online shopping	93 (65.5%)	49 (34.5%)	0.165	0.049*
Downloading media	119 (83.8%)	23 (16.2%)	0.080	0.889
Online education service	80 (56.3%)	62 (43.7%)	0.004	0.965

*significant at the 5% level

(8.1) Usage of internet banking

Within the 142 respondents, 44 (31%) did not using internet banking while 98 (69%) were using the internet banking. The Chi-square test showed that there is no significant relationship between the usage of internet banking and fraud occurrence in China because the sig. value is 0.486 and suggests that internet banking users are not at higher risk of internet fraud occurrence than non-users in China.

(8.2) Usage of online shopping / frequency of usage of online shopping

49 out of 142 (34.5%) respondents were not using online shopping and 93 (65.5%) respondents were using online shopping. Also, the Chi-square test suggested that a significant positive relationship at the 5% level between the usage of online shopping and fraud occurrence (sig. value is 0.049, correlation value is 0.165). It suggests that online shopping users are at higher risk of internet fraud occurrence in China.

(8.3) Usage of downloading media

23 (16.2%) out of 142 respondents are not downloading media from the internet and 119 (83.8%) respondents are downloading media online. No significant relationship was found between the usage of downloading media and fraud occurrence because the sig. value is 0.888 and suggests that downloading media users are not at higher risk of internet fraud occurrence than non-users in China.

(8.4) Usage of online education service

62 (43.7%) out of 142 respondents are not using online education services and 80 (56.3%) respondents are using online education services in China. We did not find a significant relationship between the usage of online education service and fraud occurrence, suggesting that online education service users are not at higher risk of internet fraud occurrence than non-users in China.

(8.5) Correlations between online activities vs. age

Table 8.9 shows the correlations between selected online activities and age. The significantly negative associations appear between age and three out of four listed online activities, these being: online shopping (r = -0.296; Sig. =0.000); internet banking (r = -0.257; Sig. = 0.002) and downloading media (r = -0.174; Sig. = 0.038). However, the use of online education services was not correlated to age (r = 0.024; Sig. = 0.776). In summary, the correlation table suggested that younger respondents are more likely to be involved in online shopping, internet banking and downloading media.

Table 8.9 also shows correlations between different online activities. Usage of online shopping is positively related to usage of internet banking (r = 0.443, sig. = 0.000); usage of online education services (r = 0.227, sig. =0.007) and also usage of downloading media (r = 0.204, sig. = 0.015). The usage of internet banking is positively related to usage online education services (r = 0.178, sig. = 0.034) and usage of downloading of media (r = 0.160, sig. = 0.057). Usage of online education services is positively related to usage of downloading media (r = 0.307, sig. = 0.000). These results are much as expected, with use of all the online activities being inversely correlated with age, which is the main driver.

Table 8.9 Spearman correlation table (online activities and age)

			usage of online shopping	usage of internet banking	usage of online education services	usage of downloading media	age
Spearman's rho	usage of online shopping	Correlation Coefficient	1.000	.443**	.227**	.204*	-.296**
		Sig. (2-tailed)	.	.000	.007	.015	.000
		N	142	142	142	142	142
	usage of internet banking	Correlation Coefficient	.443**	1.000	.178*	.160	-.257**
		Sig. (2-tailed)	.000	.	.034	.057	.002
		N	142	142	142	142	142
	usage of online education services	Correlation Coefficient	.227**	.178*	1.000	.307**	.024
		Sig. (2-tailed)	.007	.034	.	.000	.776
		N	142	142	142	142	142
	usage of downloading media	Correlation Coefficient	.204*	.160	.307**	1.000	-.174*
		Sig. (2-tailed)	.015	.057	.000	.	.038
		N	142	142	142	142	142
	age	Correlation Coefficient	-.296**	-.257**	.024	-.174*	1.000
		Sig. (2-tailed)	.000	.002	.776	.038	.
		N	142	142	142	142	142

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

8.4 Fraudulent cases

The last three survey questions in the section (3) of the questionnaire concerned personal information about actual fraud, attempted fraud and different schemes of the attempted fraud. 7 of the 142 respondents had experienced actual financial fraud and 61 respondents had experienced attempted fraud. This information is analyzed below.

8.4.1 Occurrence of attempted financial fraud

The attempted financial fraud we are referring to is the situation in which criminals tried to defraud anyone or any organization but do not succeed in causing money losses. Techniques used include spam emails, internet hijacking and virus Trojan attacks. 61 out of 142 (43%) respondents admitted that they had experienced attempted financial fraud.

The questionnaire contained six measurements to capture the frequency with which the respondent was confronted with attempts at particular types of fraud, ie Never, Yearly, Quarterly, Monthly, Weekly and Daily. Seven different types of fraud were listed.

Table 8.10 Occurrence of attempted fraud using different schemes

Fraudulent schemes	How often do you experience attempted fraud? (N=142)					
	Never	Yearly	Quarterly	Monthly	Weekly	Daily
Card cloned	100%	0	0	0	0	0
ID theft	97.2%	1.4%	0	1.4%	0	0
Scam post / junk mail	62%	7.7%	10.6%	8.5%	9.2%	2.1%
Phishing emails / spam emails	71.1%	5.6%	6.3%	5.6%	6.3%	4.9%
Fake websites / internet hijacking	88%	6.3%	1.4%	3.5%	0.7%	0
Lost / stolen bank cards	95.1%	4.2%	0.7%	0	0	0
Virus / Trojan attack	64.8%	4.2%	7.7%	9.2%	9.2%	4.9%

Table 8.10 showed that in China the least occurring attempted fraud is card cloning (0%) and the most frequent is scam post / junk mail (38%), whereas in the UK

phishing is the most frequent. The second most frequent attempted fraud is a virus / Trojan attack (35.2%), with phishing / spam emails in third place (29.9%), followed by fake websites / internet hijacking (12%). The percentages of lost / stolen card and ID theft are very close at 4.9% and 3.8%. More detailed comparison with the UK findings is left to the next chapter.

As we look at the Table 8.11, showing the correlation between the incidence of virus attack and various online activities, the statistical results indicated that in China online shopping and online education service were correlated to attempted virus / Trojan attacks.

Table 8.11 Correlation table of online activities and attempted virus / Trojan attack

Online activities	Attempted virus / Trojan attack	
	Correlation (r)	Sig. value
Usage of internet banking	0.103	0.224
Usage of online shopping	**0.211**	0.012
Usage of downloading media	0.124	0.142
Usage of online education service	**0.220**	0.009

8.4.2 Occurrence of actual financial fraud (N=7)

(1) Summary of real financial fraud

7 out of 142 respondents in China had experienced actual financial fraud, ie 4.9% of the respondents. In monetary terms, the losses suffered from each incidence of fraud ranged from RMB 10 (£1) to RMB 7800 (£780), with an average of RMB 1240 (£124). As will be discussed later, 57.2% of the defrauded customers received compensation for their loss.

(2) Time series of occurrence of fraudulent cases

The earliest fraud reported by the respondents to the survey occurred in 2004; followed by two in 2005, one in 2006, one in 2007 and two in 2008. Compared to the proportion of respondents in the UK sample that had experienced fraud, ie 21.4%, the incidence of online financial fraud in China seems not to be that serious. However, as

was made clear in the face-to-face interviews, senior professionals in the financial industry in China are concerned about the potential growth of financial fraud, particularly in relation to online transactions. Considering the big population and large market in China, event a slight increase in the occurrence of fraud could involve large monetary losses.

(3) Weekday versus weekend incidence of fraudulent transactions

For the 7 fraudulent cases collected using the survey questionnaire in China, 2 of the 7 instances (28.6%) occurred at the weekend (8am-1pm). The remaining 5 cases were spread over the other five days. Although it has not been possible to obtain any hard data on this, the opinion given in the interviews in China is that the weekend (8am-1pm) is usually the most popular time for individuals to make financial transactions including shopping and banking activities.

5 of 7 fraudulent cases involved physical presentation of bank cards / ID. It appears, from the interview discussions, that currently the majority of card fraud in China, unlike in the UK, is 'card present' fraud, particularly involving lost-and-stolen cards. Criminals obtain victim's banks card / ID illegally to start further fraud so the weekend time period tends to be targeted by criminals due to the overcrowded situation in public places, e.g. shopping malls and public transportation.

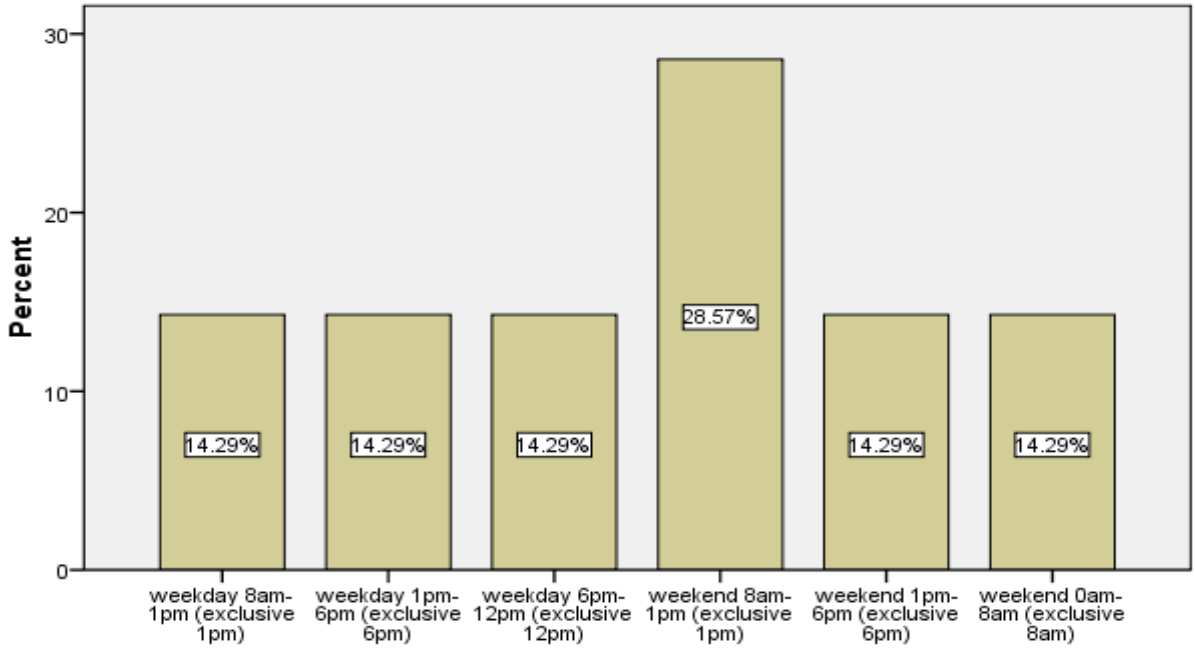


Figure 8.21 Fraudulent transactions occurrence in weekdays or weekends

(4) Where does the fraud take place?

In response to the question asking 'where do you know / believe the fraud took place', five out of the seven respondents (71.4%) believed that the fraud they experienced took place in a public place, for example, stations, stores, airports, petrol stations and bars. One respondent believed that they were defrauded at home and one believed that the fraud took place in their work place.

(5) How soon after the event was the fraud was discovered?

The table and figure below showed that 3 (42.9%) fraudulent cases were discovered within 12 hours; 1 (14.3%) was within 24 hours; 2 (28.6%) within 7 days and 1 (14.3%) within 4 weeks. Thus 4 out 7 (57.1%) fraud cases were discovered within 24 hours, the UK comparator being 36.2%. However, given the low number of actual fraud cases in China it is not possible to draw any relative conclusions about the speed of detection in the UK and China from these figures.

Table 8.12 How soon after the fraud was discovered?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	within 12 hours	3	42.9	42.9	42.9
	within 24 hours	1	14.3	14.3	57.1
	within 7 days	2	28.6	28.6	85.7
	4 weeks later	1	14.3	14.3	100.0
	Total	7	100.0	100.0	

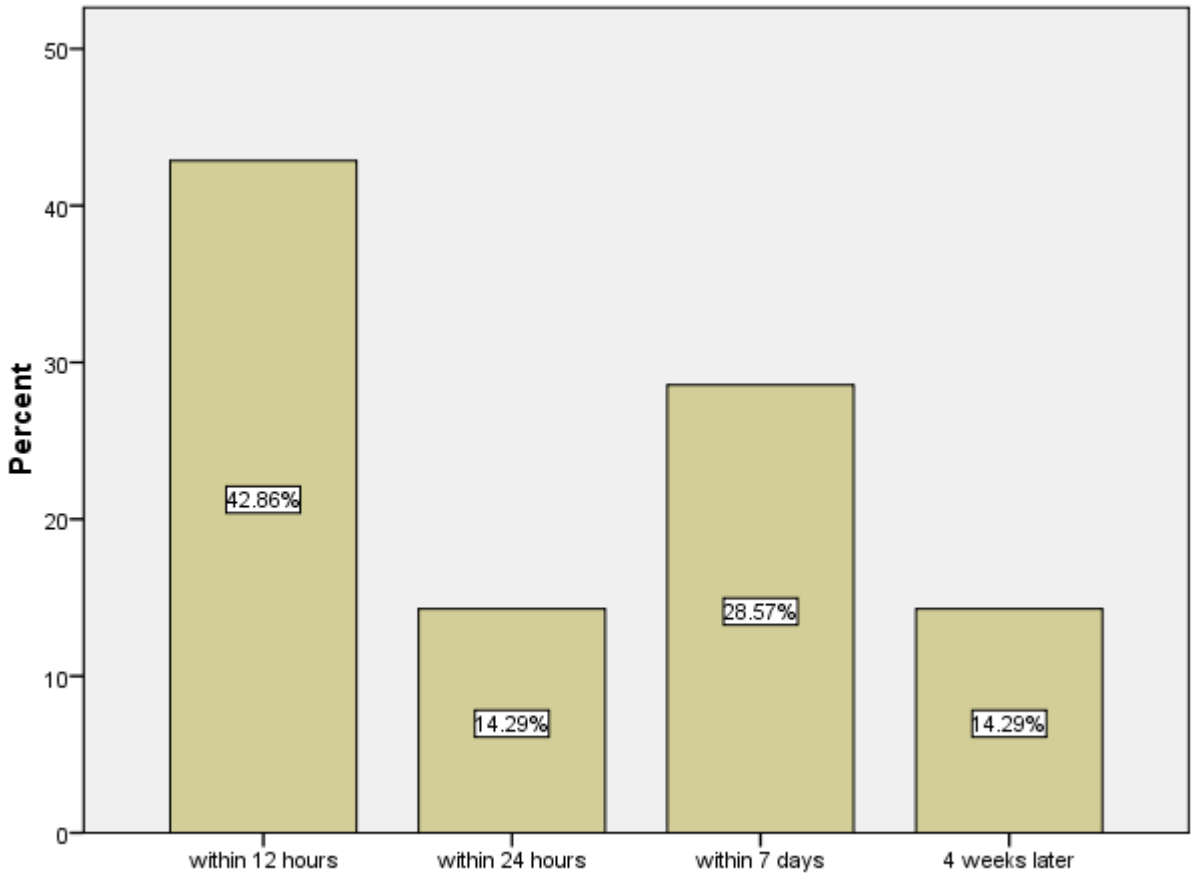


Figure 8.22 How soon after the event was the fraud was discovered?

As discussed in chapter 7, in which financial systems in China are discussed, the widespread use of mobile phone messages from the bank to the individual helps

individuals to be aware of any suspicious transactions almost in real time. In addition, local branches with staff service are open 7 days a week from 8-8 on weekdays and 9-6 on weekends, so assistance is available on a face-to-face basis. Also, self-service (no bank staff service) bank branches open 24/7 and customers can gain access to the building by swiping their bank cards. In the UK, card security services are available on a 24/7 basis by telephone but bank opening hours are more limited.

(6) Which type of fraud scheme was used?

Six most popular fraud schemes were listed: phishing email / spam emails; fake websites / internet hijacking; virus / Trojans; lost / stolen bank cards; card clone and card ID theft. Also, we provided blank space for respondent to fill in any other information if necessary. None of the seven replies was defrauded by phishing emails / spam emails which suggested that the respondents in the China survey were aware of this type of fraud scheme.

The top three fraud schemes suggested by seven respondents who had experienced actual fraud are web hijacking, lost-and-stolen card and ID theft. Two respondents (28.6%) experienced web hijacking fraud; two (28.6%) suffered from lost-and-stolen scheme and two (28.6%) were caught by card ID theft. Only one (14.3%) case occurred as the result of a card clone scheme.

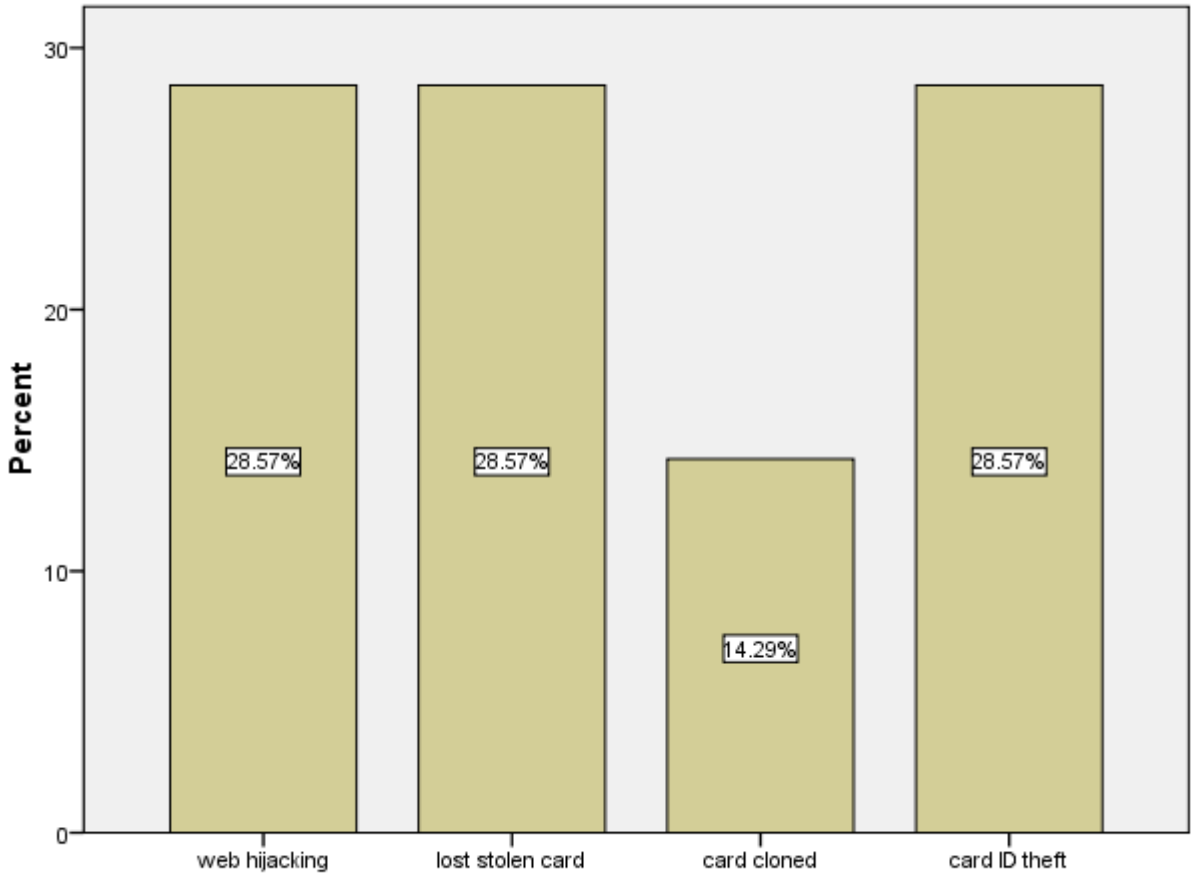


Figure 8.23 Which type of fraud scheme was used?

(7) Which type of payment method was used in this case

Five options for payment method were listed for the question asking for the payment method used for the fraud. These were: credit card; debit card; pre-paid card; cheque and secure internet payment (e.g. PayPal). Also we offered blank space to respondents to add any additional comments, but this was not used. The responses indicated that in three cases credit cards were involved and in one case a debit card.

At the end of 2009, card payments (Sohu News) constituted 25% of the volume of personal transactions in China, while in the UK the plastic card payment share reached 66.5% of total retail sales (The UK Cards Association 2010, March 2010).

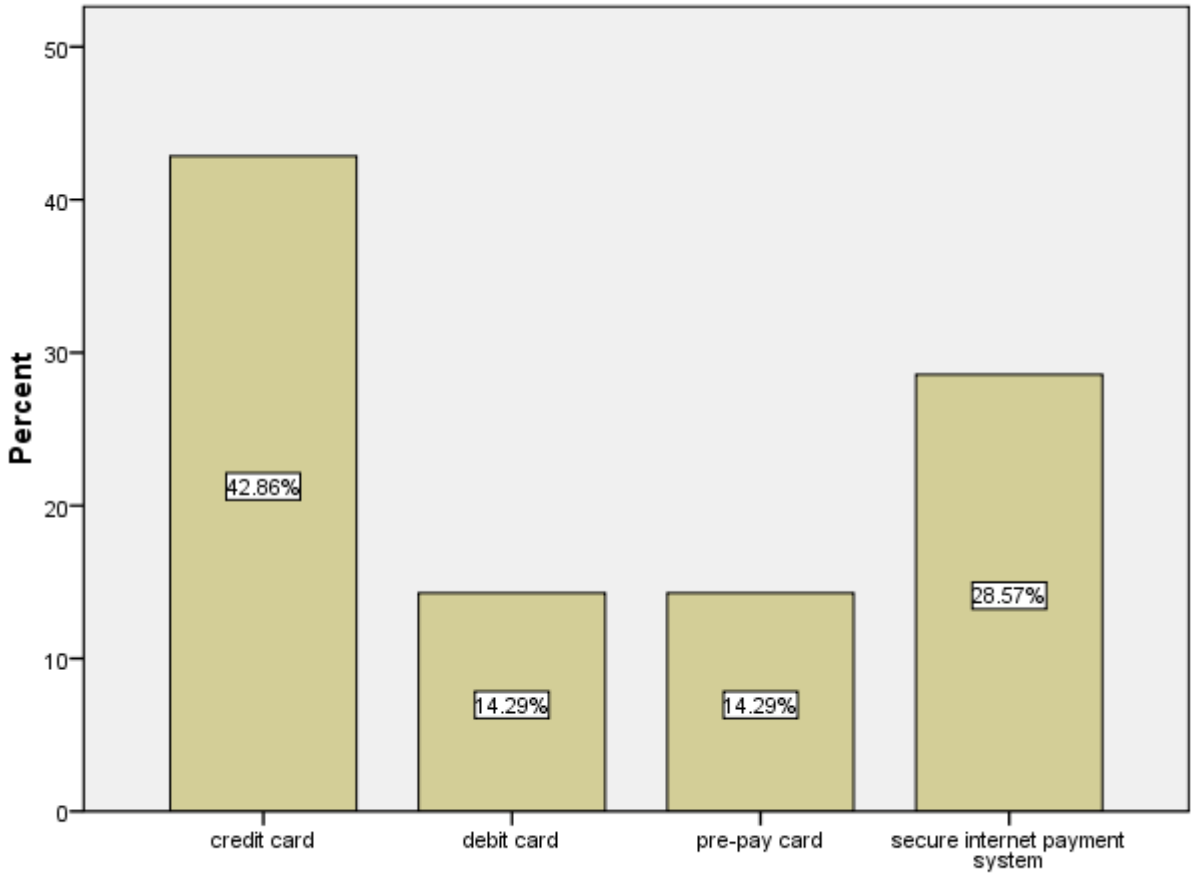


Figure 8.24 Which type of payment method was used?

(8) Did any parties compensate you?

We received 7 valid replies to the question asking whether defrauded individuals got any compensation or not. Three respondents (42.9%) got compensation from the bank or credit-card company and one respondent (14.3%) got compensation from the merchant instead. The other three respondents, whose losses were RMB 70, 30 and 120 (approximately £7, £3 and £12), did not get any compensation.

Although there is variation in practice as noted in section 3.3.4, most financial organizations in China apply a fraud claim policy which strictly limits the claim period. For example, some banks apply a 48-hour claim period starting from the time of the fraud occurrence. If customers report the fraudulent cases within this period, the banks will refund the amount immediately unless the evidence shows that customers

were involved into the fraud or acted irresponsibly. After 48 hours, refund / compensation is decided after further discussions between the individual and the bank.

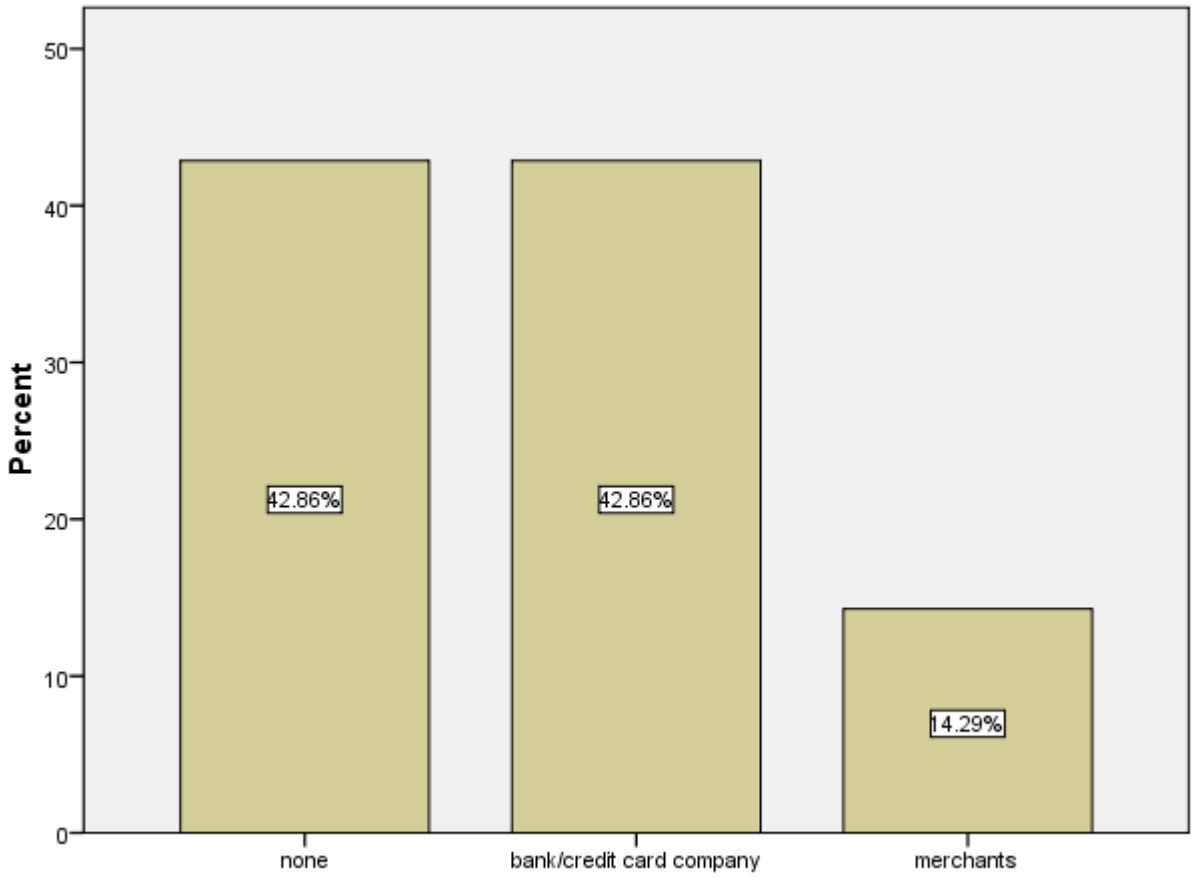


Figure 8.25 Did any party compensate you?

The professionals within the financial industry in China strongly supported the fraud refund policies currently applied. Also, they were very confident that with the latest technology, staff training and customers' education programmes, they had invested sufficiently to safeguard against widespread financial fraud in China.

(9) Awareness of different type of financial fraud

We used five scales (from 1 to 5) to measure the degree of awareness of types of financial fraud. Three out of seven defrauded respondents (42.9%) scored 'not really' to describe their awareness of types of financial fraud. two (28.6%) respondents ticked 'average' to describe their awareness of types of financial fraud.

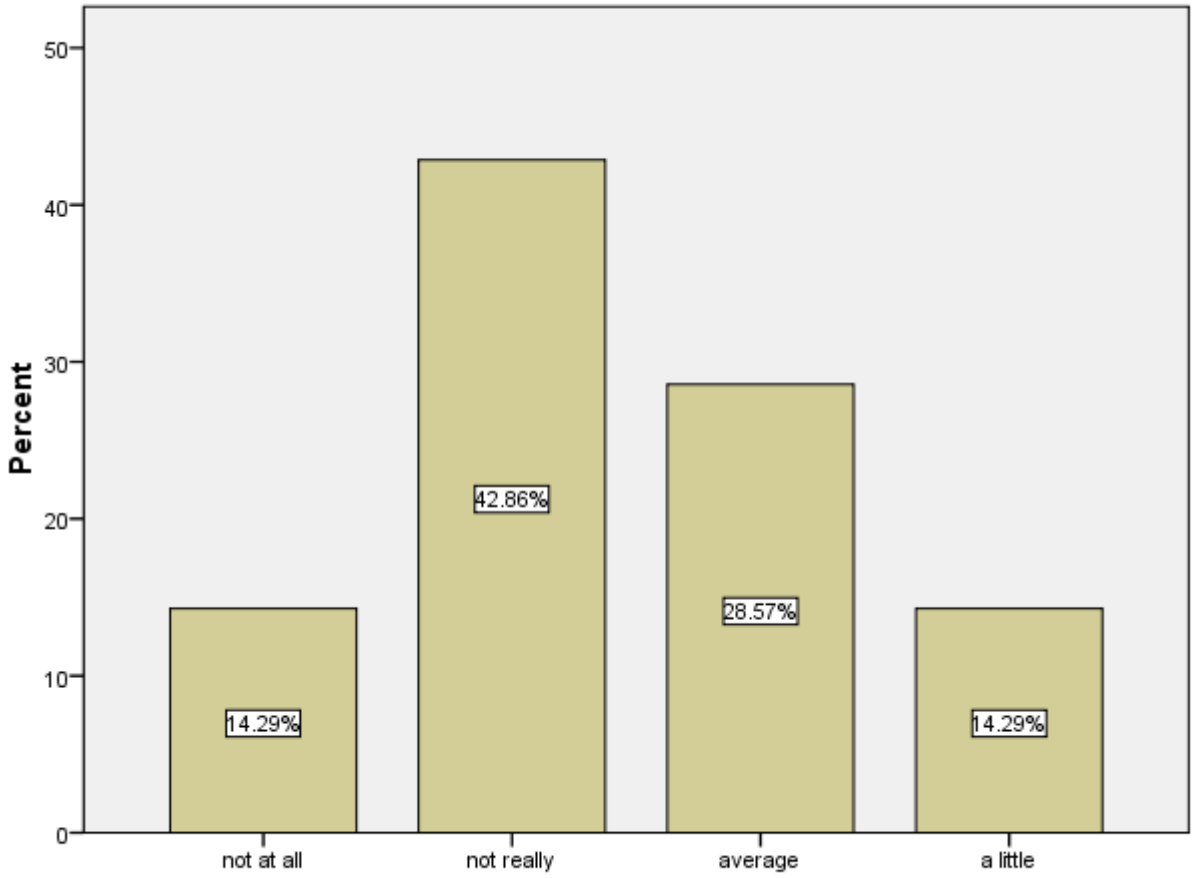


Figure 8.26 Awareness of different type of fraud

As suggested by the figure above, 57.1% of respondents in China who experienced actual fraud were still not aware of the mechanism by which they were defrauded. One explanation is that fraudulent cases rarely occur and do not get noticed by most people. Another explanation is that banks do not want to share detailed information about fraud cases with anyone, including their customers, to preserve confidentiality and business reputation. As long as customers get a fully refund, that works as a happy ending for everyone and the fraud case can be closed quietly.

(10) Satisfaction with the bank / credit card company in dealing with fraud

Considering the refund / compensation arranged by banks / credit card companies, it would be reasonable to assume that individuals who had experienced fraud should be more likely to feel satisfied with the banks / credit card companies. Although, as

before, generalizations from such as small sample could be misleading, the responses from the survey do not seem to support this view.

Five out of seven fraud cases (71.4%) scored their satisfaction with the bank / credit card company response as being below average, the other responses being just 'average'. Interestingly, two of the defrauded customers who did get compensation were nevertheless not satisfied with the way that the bank / credit card company handled the situation, possibly because of the effort they had to go through to get the compensation.

This contrasts with the responses in the UK survey, where respondents who had suffered fraud seemed very satisfied with the response of the bank / credit card company.

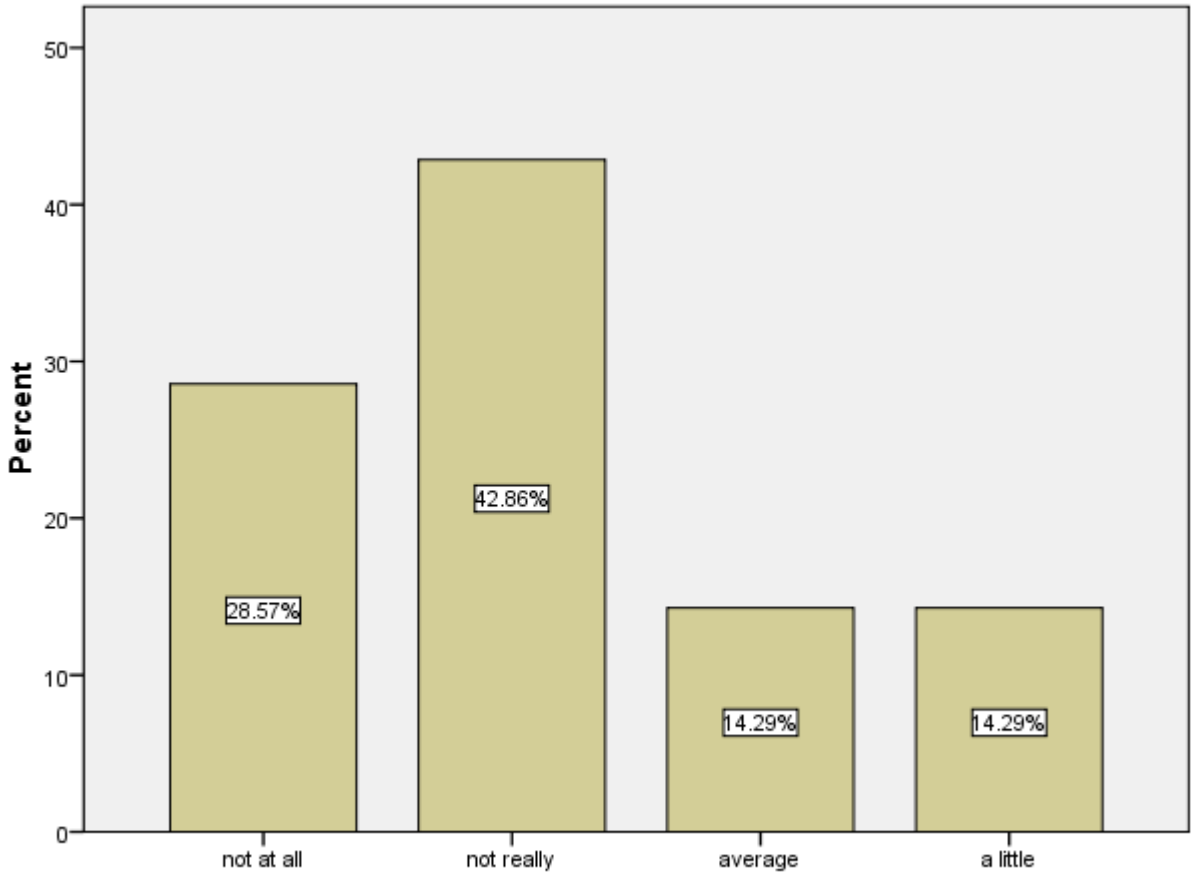


Figure 8.27 How satisfied with banks / credit card companies / in dealing with fraud

8.5 Fraud occurrence model (N=142)

In this section, we are trying to build up a model to explain and predict fraud occurrence based on the associations and correlations between different variables.

8.5.1 Tests for associations and correlations (chi-square test)

We being our more formal testing by looking at the association between pairs of variables to get a better understanding of the responses. In some cases we are looking at the correlation between the explanatory variables to explore the extent to which they are multicollinear, but generally we are looking at associations between the incidence of fraud (which is the main variable we are trying to explain) and the other variables in the survey. To accomplish this we use a Chi-square (χ^2) test to test the association, although we could also have used an F-test.

The following table shows the Chi-square test results including Chi-square value, significance value, and explanations based on the results. We use three examples to explain the table in details: firstly, we look at the row starting with general IT skills vs. age (Chi-square value = 14.317; Sig. = 0.001; r = -0.316 and sig. = 0.000). This suggests that there is a negative and significant relationship between general IT skill and age, implying that younger individuals are more likely to have better IT skills.

The Chi-square test concerning the association between usage of online shopping and fraud occurrence (Chi-square value = 3.879; Sig. = 0.049; r = 0.165 and sig. = 0.0496) is telling a different story. The r value is positive, suggesting that people who make purchase on the internet are more likely to experience fraud and the correlation is significant at the 5% level.

We could not discover any significant association between education background (IT / Finance related) and fraud occurrence (Sig. = 0.221 / 0.268). It was initially suggested that respondents who had an education background in either IT or Finance might have

an advantage in avoiding financial fraud on the internet, but this was not supported by the data.

Table 8.13 Chi-square test

Variable	Pearson	Sig.	Correlation	Sig.	Implication
General IT skill* vs. Age	14.317	0.001	-0.316	0.000	Younger respondents are more likely to have higher general IT skill
General IT skill vs. Fraud occurrence	1.686	0.430	0.076	0.366	No significant relationship was found
General IT skill vs. Highest qualification*	15.487	0.017	0.210	0.012	Respondents with higher qualification are more likely to have higher IT skills
Age* vs. Fraud occurrence	1.635	0.201	0.107	0.204	No significant relationship was found
Usage of internet banking vs. Fraud occurrence	0.485	0.486	-0.058	0.490	No significant relationship was found
Usage of online shopping vs. Fraud occurrence	3.879	0.049	0.165	0.049	Respondents who are using online shopping are more likely to be defrauded on the internet
Usage of downloading media vs. Fraud occurrence	0.020	0.888	0.012	0.889	No significant relationship was found
Usage of online education vs. Fraud occurrence	3.097	0.377	0.122	0.148	No significant relationship was found
IT/Finance related background vs. Fraud occurrence	3.018	0.221	-0.094	0.268	No significant relationship was found
General IT skill vs. Gender	0.253	0.615	0.042	0.50	No significant relationship was found
Gender vs. Fraud occurrence	1.378	0.711	0.074	0.381	No significant relationship was found
Highest qualification vs. Fraud occurrence	0.002	0.965	0.004	0.965	No significant relationship was found

*variable has been combined and recoded to avoid inaccurate test result (e.g. Age/IT skill)

8.5.2 Logistic regression model

In this section we are trying to build up a model to explain the propensity for individuals to be subjected to financial fraud. The dependent variable is therefore a limited dependent variable (LDV) or categorical variable which takes on the values zero or one depending on whether fraud has been experienced or not. According to Field, A. (2009, p265), logistic regression is multiple regression but with an outcome variable that is categorical and with predictor variables that are continuous or categorical. Similarly, the outcome variable of the model we are trying to build up is to predict fraud occurrence which is a binary variable, e.g. fraud occurrence=1; no fraud occurrence=0. Assumed predictor variables might be categorical (e.g. usage of gender / age) and numerical data (e.g. history of credit card usage).

Based on the association and correlation table in the previous section, we use 11 predictors including categorical and numerical variables to run a logistic regression. SPSS has more than one approach to test logistic regression. We chose an approach referred as 'Forward LR' by Field, A. (2009, p265) in which variables are added to the logistic equation in the order of the significance of their binary relationship with the dependent variable. The following two stages describe the progress of Forward LR test in details:

(2) Beginning block

At this stage, the initial model originates from using only the constant in the regression and tells us about the basic model included constant only. -2LL (-2 Log likelihood) in the following table represents the fit of the basic model to the data, the best fit being achieved when -2LL is minimised. As indicated by Field, A. (2009, p265), 'when including only the constant, SPSS bases the model on assigning every participant to a single category of the outcome variable'. In our study, SPSS can decide either to predict fraud occurrence or no fraud occurrence.

Table 8.14 Iteration history

Iteration History[a,b,c]			
Iteration		-2 Log likelihood	Coefficients
			Constant
Step 0	1	68.572	-1.803
	2	56.975	-2.562
	3	55.814	-2.898
	4	55.788	-2.958
	5	55.788	-2.959
	6	55.788	-2.959

a. Constant is included in the model.

b. Initial -2 Log Likelihood: 55.788

c. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

With just the constant, SPSS will predict every case into the category into which most observed cases fall. In the classification table below, there are 135 cases representing no occurrence of fraud and 7 cases representing occurrence. The chance of fraud occurrence is 7/135+7= 4.9% and the chance of fraud not occurrence is 135/135+7= 95.1%. In this simple model, with only a constant, SPSS predicts that all cases are representing the non-occurrence of fraud as this gives a higher percentage of correct classifications (100/0). As expected, this initial model correctly classified 95.1% cases.

Table 8.15 Classification table

Classification Table[a,b]					
	Observed		Predicted		
			fraud occurrence		
			not occurrence	occurrence	Percentage Correct
Step 0	fraud occurrence	not occurrence	135	0	100.0
		occurrence	7	0	.0
		Overall Percentage			95.1

a. Constant is included in the model.

b. The cut value is .500

The 'variables in the equation table' summarized the model and showed the value of the constant (b_0), which is equal to -2.959.

Table 8.16 Variables in the equation

Variables in the Equation							
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 0	Constant	-2.959	.388	58.283	1	.000	.052

In the variables **not** in the equation table, we need to focus on column sig and column score. For example, FOOAOS (frequency of usage of online shopping) has a sig. value as .013, which suggested variable FOOAOS would make a significant effect to the model if it is included in the test. FOOAOS also has the highest score value as 6.233, which would make a potential contribution to the model. Considering a significant score value, variable FOOAOS is likely to be a good predictor. In the next iteration, this variable is added to the logistic equation.

Table 8.17 Variables not in the equation

Variables not in the Equation					
			Score	df	Sig.
Step 0	Variables	FOOAOS	6.233	1	.013
		NODC	4.745	1	.029
		Overall Statistics	10.479	2	.005

(2) Method = Forward LR

Now we are looking for an improved model which gives a better fit to the data and has better classification accuracy. The procedure is repeated, with SPSS adding variables into the logistic regression one by one, on the basis of the strength of their statistical association with the dependent variable, in order to create an improved model. This is

continued until the point where adding additional variables does not add statistical significance to the model.

Continuing with our example, the model summary table below shows the overall fit of the new model through four iterations. The -2LL value of this new model has decreased from 49.575 at step 1 to 45.711 at step 2, this being less than 55.788 which was the value of -2LL in the previous basic model, showing that the model is predicting the outcome variable more accurately.

Table 8.18 Model summary (forward LR)

Model Summary			
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	49.557[a]	.043	.132
2	45.711[a]	.069	.211
a. Estimation terminated at iteration number 7 because parameter estimates changed by less than .001.			

Also, when we look at the Chi-square test table from the new model, we noticed that all the sig. values are less than 0.05. It suggests that overall the model predicts fraud occurrence or non-occurrence significantly better than when only the constant was included.

Table 8.19 Tests of model coefficients (forward LR)

Omnibus Tests of Model Coefficients				
		Chi-square	df	Sig.
Step 1	Step	6.231	1	.013
	Block	6.231	1	.013
	Model	6.231	1	.013
Step 2	Step	3.847	1	.050
	Block	10.077	2	.006
	Model	10.077	2	.006

Similarly to the basic model in previous section, the classification table describes how well the model classifies the cases overall. The basic model with only a constant correctly classifies 95.1% cases by classifying all outcomes as a non-occurrence of fraud. The revised model unfortunately does not fare any better, as all the cases of occurrence of fraud are predicted as being non-occurrences.

Table 8.20 Classification table (forward LR)

Classification Table[a]

			Predicted		
	Observed		fraud occurrence		
			non occurrence	occurrence	Percentage Correct
Step 1	fraud occurrence	not occurrence	135	0	100.0
		occurrence	7	0	.0
		Overall Percentage			95.1
Step 2	fraud occurrence	not occurrence	135	0	100.0
		occurrence	7	0	.0
		Overall Percentage			95.1

a. The cut value is .500

Now we are focusing on the table of variables in the equation. In this table, we can get the estimates for the coefficients for the predictors included in the model. For example, at the step 1, variable FOOAOS is added into the model to predict fraud occurrence or not. The coefficient of FOOAOS is .598 and sig. value is .024 which is significant. It suggested that variable FOOAOS is a good predictor in the model. With the coefficient of the constant is -4.538 at step 1, we can format the equation of the step 1 model.

Finally, we need to explain the last crucial value in the table of variables in the equation. Exp(B), generally speaking, it suggests a positive relationship between predictor and outcome if the value is greater than 1. On the other hand, a negative relationship occurs when the value is less than 1. Two predictors at the step 2,

FOOAOS (frequency of usage of online shopping) and NODC (number of debit cards) have the values of Exp(B) bigger than 1, suggesting positive relationships between FOOAOS vs. fraud occurrence and NODC vs. fraud occurrence.

Table 8.21 Variables in the equation (forward LR)

Variables in the Equation									
		B	S.E.	Wald	df	Sig.	Exp(B)	95.0% C.I.for EXP(B)	
								Lower	Upper
Step 1[a]	FOOAOS	.598	.266	5.073	1	.024	1.819	1.081	3.062
	Constant	-4.538	.973	21.769	1	.000	.011		
Step 2[b]	FOOAOS	.615	.273	5.072	1	.024	1.850	1.083	3.159
	NODC	.356	.177	4.072	1	.044	1.428	1.010	2.018
	Constant	-6.012	1.358	19.601	1	.000	.002		

a. Variable(s) entered on step 1: FOOAOS.

b. Variable(s) entered on step 2: NODC.

Based on the best model selected by SPSS using logistic regression test, we have two predictors with significant performance: FOOAOS (frequency of usage of online shopping) and NODC (number of debit cards). Both of them have positive relationships with model outcome. However, as stated earlier, the inclusion of these variable might improve model fit but it does not improve classification accuracy, so the results should be treated with care.

8.6 Conclusion

In this chapter, we have undertaken a progressive analysis of China survey data obtained, starting first with a descriptive approach, then looking at binary associations of the variables and then using logistic regression to try to explain and classify the occurrence of fraud. A number of both similarities and differences have been found in comparison with the comparable UK survey. These are explored in the next chapter.

Chapter 9 Comparison of UK and China Surveys

9.1 Introduction

In this chapter, we compare the data analysis results from the data collected in the UK and China to emphasise the difference of customers' behaviour and attitudes to the online financial transactions and internet fraud.

9.2 Comparison of the results of data analysis between the UK and China

As the same approach when we discussed SPSS results in previous chapters (chapter 6 and chapter 8), the following sections show the contrast of SPSS results from the data collected in the UK and China.

9.2.1 Data summary (UK and China)

In this section, we focus on the contrast of data summary of both UK and China, using tables to show the comparison in details and following the order as the score of general IT skills; age; usage of bank cards; customers' satisfaction; usage of online activities and attempted fraud occurrence.

(1) Score of general IT skills

The table of responses for self assessment of IT skills for the UK and China was as shown in Table 9.1 below.

Table 9.1 Score of general IT skills (UK and China)

Score of general IT skill	UK	China
Very poor	13.65%	4.23%
Poor	4.06%	1.41%
Not good	7.38%	7.04%
Average	28.78%	51.41%
Good	20.66%	22.54%
Very good	19.56%	9.15%
Excellent	5.90%	4.23%
Total	271 (100%)	142 (100%)

One can use this table to infer that 87.32% of respondents from China scored their general IT skills as average to excellent (good, very good and excellent), the corresponding figure for the UK being 74.91%. To test whether or not this difference is significant, we conduct a paired t-test under the null hypotheses (a) that the difference is significant, and (b) that the self assessment of the IT skills in the range Average to Excellent in the population from which the China sample is drawn is higher than the corresponding proportion in the UK. This test will be shown in detail in this instance. For subsequent paired t-tests the results will be shown but, given the similarity of the structure of the test, the detail as shown below will not be repeated.

(a) $H_0 : p_{china} = p_{uk}$ (b) $H_0 : p_{china} > p_{uk}$

$H_1 : p_{china} \neq p_{uk}$, $\alpha = 0.05$ (ie 5% significance)

$$s.e. = \sqrt{\frac{p_1 q_1}{n_1} + \frac{p_2 q_2}{n_2}}, \quad and \; t = \frac{p_1 - p_2}{s.e.}$$

where 1 = China and 2 = UK.

The sample data were:

$n_1 = 142$, $n_2 = 271$, $p_1 = 0.8732$, $p_2 = 0.7491$

from which

s.e. = 0.384, and t = 3.23

The critical t statistics with $n_1 + n_2 - 2 = 311$ degrees of freedom are, to two decimal places, the same as for the normal distribution with the high value of degrees of freedom in this test, the critical values being $| t_{sample} | > 1.96$ for a two tailed test (ie against null hypothesis (a)) and $t_{sample} > 1.64$ for a one tailed test (ie against null hypothesis (b), where we are testing that the self assessment of IT skills from Average to Excellent is higher in China than in the UK).

The conclusion is therefore that both for the two-tailed and the one-tailed test H_0 should be rejected – ie the self assessment of IT skills in China and the UK from Average to Excellent are different (two tailed test, hypothesis (a)), and also that the self assessment of IT skills in China from Average to Excellent is higher than the comparable proportion in the UK (one tailed test, hypothesis (b)).

This test has only looked at the scores of Average to Excellent. However, it would have been possible to have combined other categories (for example Good to Excellent) and to have conducted a similar test. Had this been done, the proportions of Average to Excellent from both samples turns out to be $p_{china} = 0.3952$ and for $p_{uk} = 0.4612$, ie the proportion in the UK sample is actually higher and significant from the China proportion at the 5% level ($t = 1.961$). The reason for this apparent anomaly is that the proportion of the respondents from China scoring their skills as Average is almost twice that of the UK. Once you take this out by only looking at Good to Excellent you get a different story. This example shows that it is important not to over-generalise the conclusions – for example not to conclude, from the first test that 'IT skills in general are higher in China'. There is also the problem that what one group might consider as average is not necessary the same as for the other group. Thus any pairwise comparison must be treated with care. It does not mean that comparisons are invalid – it means that the implications need to be looked at critically.

An alternative way of testing the difference in self-assessed IT skills is to use a chi-square test on all the categories. Using the UK proportions to calculate the expected frequencies for the China sample, the χ^2 statistic is 45.8 against a critical value at the 5% level of significance of 11.07. Therefore, there is good reason to reject the

hypothesis that the levels of self-assessed IT skills in China and the UK are same. The key differences, looking at the table, are that the UK results are more spread out, with the UK 'Very poor' category being 9.4% higher than the Chinese on, the China 'Average' being 22.6% higher and the UK 'Very good' category being 10.41% higher. The suggestion is that the China sample is more homogenous.

One factor which might be driving the differences in self assessment of IT skills is the difference in ages, which is discussed in the next section.

(2) Age

The age distribution of the two samples is shown in Table 9.2 below.

Table 9.2 Age (UK and China)

Age	**UK**	**China**
<20 Years	0.74%	0
21-30 Years	8.12%	52.11%
31-40 Years	11.81%	37.32%
41-50 Years	21.03%	7.04%
51-60 Years	17.71%	3.52%
61-70 Years	18.45%	0
>71 Years	22.14%	0
Total	271 (100%)	142 (100%)

As can be seen from Table 9.2, 52.11% of respondents from China were at 21-30 age range compared to 8.12% for the UK, while 40.59% of individuals in the UK were aged at 61-70 and >71 years, there being no respondents from China in these last two age categories. A chi-square test showed that the difference in ages was highly significant, the age distribution of the respondents from China being younger than that of the respondents in the UK. Therefore, it explains that the higher confidence of general IT skills shown in the data collected in China instead of the UK because younger individuals are more likely to have higher IT skills.

In looking at the responses from the countries individually, in both cases there was a highly significantly negative correlation between self-assessed IT skills and age (sections 6.3-(1)-(1.1) and 8.3-(1)-(1.1)). It might have been expected therefore that the younger China sample would have rated their IT skills more highly in comparison to the UK sample, but this did not seem to be the case (although as mentioned earlier it is not obvious that they would have used, implicitly, the same reference group in making their assessments). This might suggest that, in China, IT skills as a whole are at an earlier stage of development.

Other age related factors that were significant in the individual correlations were, for the UK, online shopping, internet banking, online education service and downloading media (all negative). The results for China were similar except that online education services were not significant, presumably because they are at an earlier stage of development. There is clearly an inverse relationship between the use of online services and age in both countries, as one might expect.

(3) Usage of credit card and debit card

The average number of cards and years of card usage were appreciably different in the UK and China as can be seen in Table 9.3 below.

Table 9.3 Usage of bank cards (UK and China)

Usage of bank cards	UK		China	
	Credit card	**Debit card**	**Credit card**	**Debit card**
Average number of cards	1.79	1.63	2.68	3.32
Years of card usage	19.36	18.1	4.13	8.13

Both in terms of credit cards and debit cards, the average number per person in China is almost twice that of the UK, perhaps surprisingly so as the years of card usage show the UK to be much higher than China. As was mentioned briefly in chapter 8 (8.3-(6)-(6.1)), in China, often specific cards qualify for discounts in specific outlets, and therefore to maximise their total discounts people carry more cards.

(4) Satisfaction with credit card and debit card services

Table 9.4 shows the levels of satisfaction with credit and debit cards in the UK and China.

Table 9.4 satisfaction of bank cards (UK and China)

Customers' satisfaction	UK		China	
	Credit card	**Debit card**	**Credit card**	**Debit card**
Not satisfied at all	0%	0.75%	2.96%	1.42%
Not satisfied	2.69%	1.13%	10.37%	6.38%
average	21.08%	9.77%	39.26%	43.26%
satisfied	45.29%	43.98%	36.30%	39.01%
Very satisfied	30.94%	44.36%	11.11%	9.93%

For both credit cards and debit cards, the respondents from the UK seemed more satisfied than the respondents from China, with the 'satisfied' and 'very satisfied' responses in the UK being 76% for credit cards and 88% for debit cards, the corresponding figures for China being only 47% and 49%. Looking at the two not satisfied categories, the 'not satisfied' and 'not satisfied at all' categories for the UK amounted to less than 3% for credit cards and less than 2% for debit cards, the corresponding figures for China being 13% and 8%. As mentioned in chapter 8, in China a defrauded customer cannot count on being reimbursed by the bank or credit card company. However, this might only be part of the explanation, because in China the incidence of fraud is much lower than in the UK, so the reason is more likely to be related to charges for interest, fees etc (chapter 8, section 8.3-(6)/(7)).

(5) Usage of online activities

Table 9.5 shows a similar profile for the UK and China in respect to internet banking and online shopping (although internet banking seems to be more popular amongst the China respondents).

Table 9.5 Usage of online activities (UK and China)

Online activities	**UK**		**China**	
	Yes	No	Yes	No
Internet banking	57.2%	42.8%	69%	31%
Online shopping	67.2%	32.8%	65.5%	34.5%
Downloading media	28.4%	71.6%	83.8%	16.2%
Online education services	26.9%	73.1%	56.3%	43.7%

There are significant differences, however, in the downloading of media (where China is very high) and the use of online educations services (where the UK is appreciably higher). The downloading of media effect in China is probably age related (the Chinese respondents being younger) although the evidence in chapter 8 (8.3-(8)-(8.3)), on the relation between age and downloading is not significant at the 5% level, although it is of the expected negative sign. The use of online education facilities reflects the fact that in China this is in its infancy.

(6) Incidence of attempted fraud

Table 9.6 below gives an analysis of the frequency of various methods of attempted fraud in the UK and China.

Table 9.6 Attempted fraud occurrence (UK % / China %)

Fraudulent schemes	How often do you experience attempted fraud (%)? (UK/ China)					
	Never	Yearly	Quarterly	Monthly	Weekly	Daily
Card cloned	94.8 / 100	5.2 / 0	0 / 0	0 / 0	0 / 0	0 / 0
ID theft	97.8 / 97.2	1.5 / 1.4	0 / 0	0.4 / 1.4	0 / 0	0.4 / 0
Scam post / junk mail	65.3 / 62	4.4 / 7.7	3.7 / 10.6	9.2 / 8.5	11.8/ 9.2	5.5 / 2.1
Phishing emails / spam emails	62.0 / 71.1	4.8 / 5.6	7 / 6.3	4.4 / 5.6	13.7/ 6.3	8.1 / 4.9
Fake websites / internet hijacking	86.7 / 88	3.3 / 6.3	3.3 / 1.4	3.7 / 3.5	1.5 / 0.7	1.5 / 0
Lost / stolen bank cards	93.7 / 95.1	5.9 / 4.2	0 / 0.7	0.4 / 0	0 / 0	0 / 0
Virus / Trojan attacks	80.8 / 64.8	8.9 / 4.2	4.1 / 7.7	3.3 / 9.2	1.8 / 9.2	1.1 / 4.9

The main features of Table 9.6 are (i) the percentages in the 'never' column are similar for the UK and China, except for 'virus / Trojan attacks', which seem to be

more prevalent in China, (ii) the frequency of most of the problems seems to be a little lower in China, as a rule, except again for virus and Trojan attacks, and (iii) the incidence of 'phishing emails' tends to be a little lower in China, possibly because the language abilities of the Eastern European sources from which many phishing attacks emanate does not stretch to Mandarin.

9.2.2 Correlation table (UK and China)

Only three significant correlations were found for China: general IT skill vs. age (-ve); general IT skill vs. highest qualification (+ve) and usage of online shopping vs. fraud occurrence (+ve). For the UK, these correlations were also found to be significant, but in addition, the following correlations were also significant: general IT skill vs. fraud occurrence (+ve) ; general IT skill vs. highest qualification (+ve); usage of internet banking vs. fraud occurrence (+ve); and usage of downloading media vs. fraud occurrence (+ve). These are relationships are unsurprising with the possible exception of the significant positive correlation, in the UK only, between IT skill and fraud occurrence, where the maintained hypothesis might be that those people with high IT skills might be less susceptible to fraud. For China, the relationship is also positive but not significant. For the China data, the incidence of actual fraud (7 cases) was too low for correlations with fraud occurrence to be statistically significant, with the possible exception of the positive association between online shopping and fraud occurrence if viewed as a one-tailed test (ie the null being that the correlation was greater than zero, as opposed to non equal to zero).

Although the same survey questionnaire (apart from the language difference) was used in both the UK and China, delivery and collection methods were slightly different due to the local rules and culture. We received 271 valid replies (58 fraudulent cases included) in the UK and 142 valid replies in China. One reason behind the less significant associations in the China data is therefore due to the lower number of responses driving up the standard errors in the hypothesis tests. A second factor, which is particularly important when looking at correlations with incidents of fraud, is the low number of fraud cases in China.

Table 9.7 Table of the correlation and sig value (UK and China)

Variable	UK		China	
	Correlation	Sig.	Correlation	Sig.
General IT skill* vs. Age	-0.601	0.000**	-0.316	0.000**
General IT skill vs. Fraud occurrence	0.168	0.004**	0.076	0.366
General IT skill vs. Highest qualification*	0.202	0.001**	0.210	0.012**
Age* vs. Fraud occurrence	-0.108	0.076	0.107	0.204
Usage of internet banking vs. Fraud occurrence	0.215	0.000**	-0.058	0.490***
Usage of online shopping vs. Fraud occurrence	0.212	0.000**	0.165	0.049
Usage of downloading media vs. Fraud occurrence	0.210	0.001**	0.012	0.889
Usage of online education vs. Fraud occurrence	-0.053	0.383	0.122	0.148
IT/Finance related background vs. Fraud occurrence	0.012	0.839	-0.094	0.268
General IT skill vs. Gender	0.106	0.082	0.042	0.50
Gender vs. Fraud occurrence	-0.097	0.110	0.074	0.381
Highest qualification vs. Fraud occurrence	0.097	0.109	0.004	0.965

*variable has been combined and recoded to avoid inaccurate test result (e.g. Age/IT skill)
** significant at the 5% level (2 tailed-test against the null hypothesis that the correlation is zero)
*** significant at the 5% level (1 tailed-test against the null hypothesis that the correlation is greater than zero)

9.2.3 Logistic regression model (UK and China)

Based on the associations discovered in previous sections, we now attempt to find out if there is any further relationship that can be established to predict fraud occurrence using logistic regression. Table 9.8 summarizes the results obtained in chapters 6 and 8 from the logistic regressions on the UK and China data respectively. This shows that four predictors (UOOAIB, UOOAOES, UOOADM and HUDC) performed significantly in the UK model and only two (FOOAOS and NODC) in China model.

Table 9.8 Table of the significant predictor variables in the logistic equations (UK and China)

Variables	UK (4)	China (2)
UOOAIB (usage of internet banking)	Y	N
UOOAOES (usage of online education service)	Y	N
UOOADM (usage of downloading media online)	Y	N
HUDC (history of usage of debit card)	Y	N
FOOAOS (frequency of usage of online shopping)	N	Y
NODC (number of debit cards owned)	N	Y

The conclusion from the table is that there is no obvious consistency between the logistic regressions to predict the occurrence of fraud between the UK and China. This is not particularly surprising. With only seven cases of fraud in the China sample, any logistic regression to capture the determining factors is likely to be unstable as there is likely to be a strong random element to these (rare) incidents. On the other hand, with 58 incidents of fraud in the UK sample, the logistic regression is more robust, even if the Nagelkirke r^2 is still modest at 0.205.

9.3 Conclusion

In this chapter, we provided a comparison of the findings from the UK and China samples based on the statistical results obtained from SPSS. In the next chapter, we draw together the main findings to conclude our study and provide further approaches for future research related to this topic.

Chapter 10 Conclusions

10.1 Introduction

In this final chapter in the thesis, we summarise and reflect on the main findings of this study and suggest research directions for future research.

10.2 Summary of this study

This thesis is entitled 'an investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China'. This is an important question because, at the present point in time, there is an uneasy equilibrium between the increasing sophistication and cunning of the fraudsters versus the attempts by programmers, systems experts, database designers and others to tackle this increasing menace. It is no exaggeration to say that the future of online financial transactions is in the balance. There are systems experts who refuse to have an online bank account because, in their judgement, there is currently an insufficient level of security to provide them with the level of trust necessary for them to be confident that their money is not at risk.

The central question at the heart of this dissertation, as outlined in chapter 1 (section 1.3) and chapter 2 (section 2.7) is to explore both the susceptibilities and the attitudes of individuals to electronic fraud in relation the statistical data, the surveys undertaken in this study, the robustness of the electronic systems and the responsiveness and 'user friendliness' of the financial institutions in matters such as compensation and willingness to help. As discussed in chapter 2 (particularly section 2.6), there are few academic studies in this area, with most of the attention being directed at the attitudes of consumers to internet banking rather than to fraud, and no studies dealing directly with actual cases of fraud. It was to this gap in the literature that the study was addressed.

The main findings from the UK survey were: younger respondents are more likely to have higher general IT skill; respondents with higher IT skill are more likely to be

defrauded on the internet; respondents with higher qualifications are more likely to have higher IT skill; younger respondents are more likely to be defrauded on the internet. Also, certain types of online activities present higher risks of fraud to the respondents who are using internet banking; online shopping and media downloading. Furthermore, four predictors (usage of internet banking, usage of online education services, and usage of downloading media and length of debit card usage) were significant factors in the logistic regressions used to classify fraud occurrence / non-occurrence in the UK. Most of these are in line with expectations, although it might be expected that those with higher IT skills would be less susceptible to fraud rather than more susceptible. Of particular interest was the generally high degree of customer satisfaction with the banks / card companies from those who had been defrauded. This is important: it points to there being a strong commitment on behalf of these companies to maintain consumer confidence rather than try to avoid providing assistance and/or compensation when things go wrong.

From the China survey, statistically significant findings, much in line with expectations, were that younger respondents are more likely to have higher general IT skill; and respondents with higher qualifications are more likely to have higher IT skill. However, online shopping was the only online activity which was significantly correlated to fraud occurrence. Finally, the two significant explanatory variables in the logistic regression to categorize fraud occurrence / non-occurrence were frequency of usage of online shopping and number of debit cards. Neither of these was selected in the UK logistic regression, although it is interesting that there is a variable related to debit cards in each final model. In analysing the actual cases of fraud, one finding of interest was a lower level of satisfaction with the banks when actual fraud had occurred in comparison to the UK, although the incidence of fraud in the sample was lower.

In looking at cases of attempted fraud, the main comparisons were that virus and Trojan attacks seem to be more prevalent in China, but the incidence of phishing attacks were lower, possibly (as explained in chapter 8) because the Eastern European exponents of phishing, who provide much of the phishing email in the UK, have more of a language barrier when it comes to directing such attacks at China.

10.3 The Future of Electronic Transactions

The banks and credit card companies have considerable financial gains to be made out of electronic transactions. Operating in a virtual medium, with low infrastructure costs, means that there are very significant savings to be made. High street branches and the associated staffing levels are costly to maintain: online transactions reduce the transactions costs considerably. Even if online transactions are more susceptible to fraud, it is in the banks' interests to reimburse customers to maintain confidence in this transactions medium, provided the costs of fraud are kept to an acceptable level. This is also true of credit cards. The losses from 'card-not-present' transactions, as discussed in chapter 4, are high, but credit card operations are highly profitable and provided the companies can recover their losses through charging high merchant fees and high rates of interest on unpaid balances, they will continue to be profitable. It is therefore in their interests, at least at current fraud levels, to reimburse customers for actual occurrences of fraud. This was evidently the situation evidenced by the UK survey, where customer satisfaction levels with the banks responses to dealing with fraud were high, but this was less evident in China, although actual fraud levels were lower.

From time to time there is a technological breakthrough which shifts the balance of power between the banks and the fraudsters. Sophisticated viruses, worms and Trojans have given power to the fraudsters, whereas the introduction of Chip-and-PIN technology in 2004 greatly reduced the number of fraudulent POS transactions in UK retail outlets. However, not all countries have adopted Chip-and-PIN, so cross-border transactions are still vulnerable, and many cloned credit cards end up being used in non Chip-and-PIN environments such as Australia or the United States.

Some vulnerabilities however are difficult to eliminate; card-not-present transactions in particular fall into this category. The response of credit card companies to online transactions of this nature is to profile customers to try to detect transactions that are out of character. For example, if an individual tends to make online shopping purchases during normal daytime hours, an internet gaming transaction at 3am will be

picked up immediately and the chances are the transaction will be refused. A second line of defence is the increasing use of 'secure' systems discussed in chapter 2, where the bank or credit card company requires an additional layer of authorization before the transaction is processed (eg NatWest Secure, MBNA Secure etc).

However, with card-not-present transactions over the telephone or by mail order, the situation is not so reassuring as the policing systems described above are not employed. Providing the banks / credit card companies can recover the costs of reimbursing fraudulent transactions, these forms of payment will probably continue to operate. However, any material shift in the ability of the fraudsters to exploit the weaknesses may result in these means of payment being discontinued. It is still the case that the simplest fraud schemes net the most profits overall, and as seen from both the survey data and the APACS statistics in chapter 4, simple card cloning is still high on the list as a major source of fraudulent transactions, even though Chip-and-PIN has helped to control this domestically although it is understood that fraudsters now have the technology to clone the chips embedded in the cards.

Finally, what about the security of internet banking? Careful use of this transactions medium over a private encrypted network should provide good security, but it is still vulnerable, particularly where individuals write down their passwords and these could then be stolen. With the recent tendency to require individuals to have ever more complex passwords, the capacity for them to be remembered easily diminishes. In addition, more technical vulnerabilities to worms, Trojans etc mean that 100% security cannot be guaranteed, at least not with current technology. However, the cost savings to the banks will ensure that every effort is made to make online banking secure.

10.4 Future research

The research experiences gained from this study suggest a number of areas for future research, particularly into the under-researched area of fraud. Rather than approach the research questions through individuals, there would be much value in working with merchants and financial organizations that are dealing with financial transactions

and fraud on daily basis. In conducting this study, we approached a number of banks in the UK including HSBC, NatWest and American Express, but they were reluctant to give out any information or agree to meetings because of its commercial and technical sensitivity. However, we succeeded in getting three interviews with banks in China, although they asked to remain anonymous. If a researcher could get around this veil of secrecy, there would be much interesting information and data to analyze. It is hoped that the author of this thesis will be able to conduct research of this nature in the future. If this could be done internationally, the study would be particularly interesting.

One other area of interest would be to investigate the financial models of the banks and credit card companies to see what assumptions and allowances they factor in for fraud. Again, this information is likely to be highly commercially sensitive and the likelihood of being able to study this area in detail is remote.

10.5 Conclusions

The key features of this study are that it has focused on the issues of actual and attempted fraud, not just in the UK but also with a parallel survey in China. The China survey was the more difficult to conduct, because for confidentiality reasons it had to be conducted through the medium of a bank. Other international surveys might experience similar problems due to differing social environments and systems for mail delivery. However, despite electronic transactions being a more recent innovation in China, the problems in terms of actual and attempted fraud were broadly similar. However, the incidence in the China survey was lower, which might suggest that some lessons had been learned and that Western systems of electronic payment had not just been copied without modification. China is at an earlier stage of development but the growth in electronic transactions is massive, so the potential for fraudsters is also huge. It will be interesting to see how the balance of power between the technologist and systems designers on the one hand and the fraudsters on the other evolves as this electronic market grows.

Appendix A: Questionnaire in both English and Chinese

Hi

I believe that financial fraud is even more common than the statistics suggest. Many of my friends have suffered from fraud both in credit card transaction and in telephone banking.

As part of my studies at Loughborough University I am carrying out a study to collect more useful information on financial fraud. If you **have** suffered problems of this type I would be grateful if you could share the details with me by completing the attached questionnaire and returning it to me in the reply paid envelope provided.

If you **have not** suffered from financial fraud, I also would be very grateful if you could fill Section (1), (2) and (3) of this questionnaire and return it to me. This survey is completely anonymous and it's impossible for you to be traced from the returned questionnaires. The more information I get, the more valuable the survey.

I hope very much you can help.

Yours sincerely

Yan Sun

- Please fill section **(1), (2), (3)** if you **have not** experienced any FINANCIAL FRAUD.
- Please fill section **(1), (2), (3) and (4)** if you **have** experienced any FINANCIAL FRAUD.

The information on this form CANNOT BE TRACED BACK TO INDIVIDUALS. Its purpose is to help with profiling cases of financial fraud to assist with its elimination.

Section (1) Basic financial information

1.1 How many CREDIT cards have you got (including joint account and corporate credit cards)? ( )

1.1a Do you use different CREDIT cards for different transaction amounts (e.g. small, medium and large)?

Yes □ No □

1.1b Do you use different CREDIT cards for different purposes (e.g. household, petrol and holiday)?

Yes □ No □

1.2 How long have you been using CREDIT cards? ____Year(s)

1.3 How satisfied are you with your CREDIT card service so far? (Circle the most appropriate level)

Not satisfied at all Very satisfied

1 2 3 4 5 Level

1.4 How many DEBIT cards have you got (including joint account and corporate debit cards)? ( )

1.4a Do you use different DEBIT cards for different transaction amounts (e.g. small, medium and large)?

Yes □ No □

1.4b Do you use different DEBIT cards for different purposes (e.g. household, petrol, and holiday)?

Yes □ No □

1.5 How long have you been using DEBIT cards? ____Year(s)

1.6 How satisfied are you with your DEBIT card service so far? (circle the most appropriate level)

Not satisfied at all Very satisfied

1 2 3 4 5 Level

1.7 How many different personal banking channels have you been using (tick as appropriate)?

Branch banking	□
Postal banking	□
Internet banking	□
Telephone banking (staff involved)	□
Auto Tele. Banking (e.g. Actionline)	□

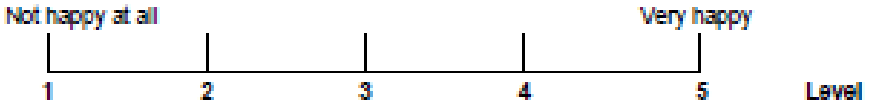
1.8 How long have you been using different banking channels?

Branch banking	_____Year (s)
Postal banking	_____Year (s)
Internet banking	_____Year (s)
Telephone banking (staff involved)	_____Year (s)
Auto Tele. Banking (e.g. Actionline)	_____Year (s)

1.9 How often do you use different banking channels per month?

Branch banking	_____/ Month
Postal banking	_____/ Month
Internet banking	_____/ Month
Telephone banking (staff involved)	_____/ Month
Auto Tele. Banking (e.g. Actionline)	_____/ Month

1.10 Increasingly websites are demanding that you have more complicated passwords with a combination of numbers and letters, are you happy with this? (circle the most appropriate level)



1.11 Would you prefer a simple password you can memorize to a complicated one that has to be written down and stored (possibly compromising its security)? (tick as appropriate)

Yes □ No □

1.12 Do you tend to use the same password / pin number wherever it is possible? (tick as appropriate)

Yes □ No □

1.13 When you manage your personal finance, do you prefer to deal with real people or an auto machine? (tick as appropriate)

Prefer real people	Cash withdrawal □	Order cheque book □	Change pin □	Money transfer □
	Cash deposit □	Balance checking □	Change address □	Personal investment □
	Regular payments (e.g. bills) □		Mortgage/ Loan service □	
Prefer an auto machine	Cash withdrawal □	Order cheque book □	Change pin □	Money transfer □
	Cash deposit □	Balance checking □	Change address □	Personal investment □
	Regular payments (e.g. bills) □		Mortgage/ Loan service □	

1.14 How often do you use the payment methods below in DOMESTIC and OVERSEAS transaction? (please give scores : 1 is the least used and 5 is the most used)

	Cash	Cheque	Credit card	Debit card	Payment online	Bank transfer
Domestic	( )	( )	( )	( )	( )	( )
Overseas	( )	( )	( )	( )	( )	( )

1.15 Are you using Chip-and-Pin for (tick as appropriate)?

Only credit card(s)	□
Only debit card(s)	□
Both credit and debit card(s)	□
Neither credit nor debit card(s)	□

1.16 Do you tend to pay off your credit cards every month? Yes □ No □

1.17 Please give score 1-7 to indicate your confidence of security in transactions using following: (1 is the least confident and 7 is the most confident)

Cheque ( )	Online banking ( )	ATM ( )	Petrol station ( )
Debit card ( )	Data encryption ( )	Chip-and-pin ( )	Merchants (e.g. shops) ( )
Credit card ( )	Internet transaction ( )	Online shopping ( )	Bank /Credit card company ( )

Section (2) IT usage information

2.1 Which item below describes the degree of your computer usage at work and at home? (tick as appropriate)

At work		At home	
Never use	□	Never use	□
limited computer experience (<1hour per day)	□	limited computer experience (< 1 hour per day)	□
Occasional work use (1-2hours per day)	□	Occasional home use (1-2 hours per day)	□
Intensive work use (> 3 hours per day)	□	Intensive home use (> 3 hours per day)	□

2.2 How many different online activities do you use (tick as appropriate)?

Online shopping □ Information search □ Internet Banking □ Online communication □

Online games/ gambling □ Online education services □ Others (please state):

2.3 How long have you been using these online activities (in Years)?

Online shopping ___Year (s) Information search ___Year (s) Internet Banking ___Year (s)

Online communication ___Year (s) Online games / gambling__Year (s) Online education services_Year (s)

Others (please state):

2.4 How often do you do these online activities per month (tick as appropriate)?

	Never	Yearly	Quarterly	Monthly	Weekly	Daily
Online shopping	□	□	□	□	□	□
Information search	□	□	□	□	□	□
Internet Banking	□	□	□	□	□	□
Online communication	□	□	□	□	□	□
Online games / gambling	□	□	□	□	□	□
Online education services	□	□	□	□	□	□

Others (please state):

2.5 Which score below best represents your general IT skills (tick as appropriate):

1 = very poor	2 = poor	3 = not good	4 = average	5 = good	6 = very good	7 = excellent
□	□	□	□	□	□	□

2.6 Have you received any IT training from (tick as appropriate)?

High school	College/ Uni.	Work	Online courses	Self-education	Prof. Qual.
□	□	□	□	□	□

Others(please state)

Section (3) Personal information

3.1 Age (tick as appropriate)

<= 20(Years)	21-30	31-40	41-50	51-60	61-70	>71
□	□	□	□	□	□	□

3.2 Gender (tick as appropriate)

Male	Female
□	□

3.3 Which item below describes your highest qualification (if known)? (tick as appropriate)

No formal qualification	GCSE/ 'O' levels	A level	BSc/BA / Prof. Qual.*	Further degrees	Not known
□	□	□	□	□	□

*Professional qualifications include commercial pilots' licences, police inspectors' examinations and attainments of similar standards as well as medical legal and accountancy qualifications.

3.4 Is your education background related to IT or Finance (tick as appropriate)?

IT related □ Finance related □ Both of them □ Neither of them □

3.5 How many incidents of ACTUAL* financial fraud have you experienced? ( )

*Actual financial fraud: fraudulent transaction has taken place and caused money losses to anyone or any organization.

3.6 Have you ever experienced ATTEMPTED* financial fraud?

Yes □ No □

*Attempted financial fraud: criminals tried to defraud anyone or any organization but not succeed in causing money loss.

3.7 How often have you experienced ATTEMPTED* financial fraud using the following fraud schemes? (tick as appropriate)

	Never	Yearly	Quarterly	Monthly	Weekly	Daily
Card cloned[1]	□	□	□	□	□	□
ID theft	□	□	□	□	□	□
Junk mail / scam post	□	□	□	□	□	□
Phishing emails[2] / spam emails	□	□	□	□	□	□
Fake websites / Internet jacking[3]	□	□	□	□	□	□
Lost / stolen bank card	□	□	□	□	□	□
Virus/ Trojans attack	□	□	□	□	□	□

Others (please state):

Would you like to spare 10 minutes for a chat by phone / email / post / in person?
If yes, please tell us how to contact you:

[1] Counterfeit card fraud occurs when an illegal copy of a genuine credit or debit card is made
[2] Phishing email attack is an attempt to trick customers of that company into disclosing information at a bogus website operated by fraudsters persuading customers to update their personal or account information by clicking links contained in emails.
[3] Online users get automatically redirected to an alternative website of the hijacker's choice without users' consent.

Section (4) Please complete this section if you have experienced any ACTUAL financial fraud

"" Please complete this section for each incidence of ACTUAL fraud you have experienced.
"" Also you can photocopy section (4) if necessary.

4.1 How much money was involved in the fraud (total losses incurred)? £_____

4.2 When did the fraudulent transaction happen (tick as appropriate)? Date: Month Year

	8am–1pm (exclude 1pm)	1pm–6pm (exclude 6pm)	6pm–12pm (exclude 12pm)	0am–8am (exclude 8am)
Weekday	□	□	□	□
Weekend	□	□	□	□

4.3 Where do you know/ believe the fraud took place (tick as appropriate)?

Work place (e.g. offices)	Public place (e.g. stations/stores/bars)	At home
□	□	□

Others (please state):_____

4.4 How soon after the fraud was the problem discovered (tick as appropriate)?

Within 12 hours	Within 24 hours	Within 7 days	2 weeks later	4 weeks later	More than 1 month
□	□	□	□	□	□

4.5 How was the fraudulent transaction discovered (tick as appropriate)?

Checking bank or credit card statements □ Credit card rejected at the check-out □

Received warning phone call from banks □ Debit card rejected at the check-out □

Received suspicious bills / purchase confirmations □ Purchased products not received □

Others (please explain):

4.6 Which type of fraud scheme was used in this case (tick as appropriate)?

Phishing emails* / spam emails □ Fake websites/ Internet jacking* □ Virus/ Trojans attack □

Lost / stolen bank cards □ Card cloned □ Card ID theft □

Others (please state):_____

* see footnotes in page 5 for an explanation

4.7 Which type of payment method was used in this case (tick as appropriate)?

Credit card	Debit card	Pre-pay card	cheque	Secure Internet payment system (e.g. PayPal /Natwest secure)	Others (please state)
□	□	□	□	□	

4.8 Did any of the following parties compensate you (tick as appropriate)?

Bank / credit card company ☐ Merchant ☐ None of them ☐ Others (please state):

4.9 Who do you think should take the most responsibility for eliminating internet fraud (tick as appropriate)?

Bank	credit card company	Merchant	Customer	Police
☐	☐	☐	☐	☐

Others (please state):

4.10 Are you going to give up or reduce your use of (tick as appropriate)?

	Online banking	Online shopping	Online communication	Online game/ gambling
Give up	☐	☐	☐	☐
Reduce usage	☐	☐	☐	☐
Neither of above	☐	☐	☐	☐

Others (please state):

4.11 How aware do you think people are of internet fraud these days? (Circle the most appropriate level)

Not at all Very much

1 2 3 4 5 Level

4.12 How satisfied were you with your bank/ credit card company in dealing with the fraudulent situation? (Circle the most appropriate level)

Not satisfied at all Very satisfied

1 2 3 4 5 Level

4.13 Through which channel were sensitive personal financial details acquired illicitly (if known)? (tick as appropriate)

Not known	By internet	By post	By telephone	By survey	By bin raid*	By purchase	By ATM
☐	☐	☐	☐	☐	☐	☐	☐

Others (please state):

*i.e. by people sifting through rubbish and finding personal details.

4.14 What types of sensitive information do you think were acquired by the fraudsters (tick as appropriate)?

Name ☐	Postal address ☐	Date of birth ☐	Telephone number ☐
Account numbers ☐	Debit card numbers ☐	Credit card numbers ☐	NI numbers ☐
Passwords / PIN number / Security words ☐		Driving licence numbers ☐	E-mail address ☐

Others (please state):

第一节 基本的个人理财信息

1.1 您拥有几张信用卡 （包括联合帐户和公司帐户） （ ）

1.1a 您是否使用不同的信用卡支付不同金额的消费 (例如：小金额，中等金额和大笔金额的消费)?

是 □ 否 □

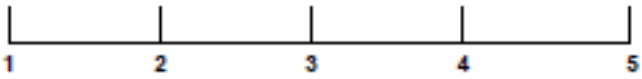
1.1b 您是否使用不同的信用卡支付不同类别的消费 (例如：日常家用，交通费用和外出旅行)?

是 □ 否 □

1.2 迄今为止，您使用信用卡的总年数？ ____年

1.3 您对于信用卡的服务满意程度是以下的哪一个等级？(在相关的数字上标志)

根本不满意 非常的满意



满意等级

1.4 您拥有几张现金卡 （包括联合帐户和公司帐户） （ ）

1.4a 您是否使用不同的现金卡支付不同金额的消费 (例如：小金额，中等金额和大笔金额的消费)?

是 □ 否 □

1.4b 您是否使用不同的现金卡支付不同类别的消费 (例如：日常家用，交通费用和外出旅行)?

是 □ 否 □

1.5 迄今为止，您使用现金卡的总年数？ ____年

1.6 您对于现金卡的服务满意程度是以下的哪一个等级？(在相关的数字上标志)

根本不满意 非常的满意

满意等级

1.7 您是通过哪几种服务方式办理个人银行/理财业务 (请在相关项标志)?

前往银行营业厅办理 □
邮寄办理方式 □
网上银行 □
人工电话办理 (人工服务) □
自动电话办理 (无人工服务) □

1.8 迄今为止，您使用过的不同的服务方式办理个人银行/理财业务的总年数 (请在相关项标志)?

前往银行营业厅办理 ____年
邮寄办理方式 ____年
网上银行 ____年
人工电话办理 (人工服务) ____年
自动电话办理 (无人工服务) ____年

1.9 您使用不同的服务方式办理个人银行/理财业务的大概频率 (以日历月为单位计算)?

前往银行营业厅办理 ____月
邮寄办理方式 ____月
网上银行 ____月
人工电话办理 (人工服务) ____月
自动电话办理 (无人工服务) ____月

1.10 您对于日益复杂的密码/用户名（例如要求您使用数字和字母的组合）的满意程度是？(在相关的数字上标志)

根本不满意 非常的满意

1 2 3 4 5 满意等级

1.11 相对于繁琐冗长的用户名/密码（需要记录下来以便查阅），您是否更加倾向于简单易记的用户名/密码（安全性少许降低）？(请在相关项标志)

是 □ 否 □

1.12 您是否乐于使用相同的用户名/密码操作任何账户？(请在相关项标志)

是 □ 否 □

2

1.13 当您需要办理个人银行/理财业务的时候，您愿意通过银行职员办理还是使用自动化的设备？ (请在相关项标志)

	现金取款 □	预定支票本 □	更改密码 □	转账 □
通过银行职员	现金存款 □	账户查询 □	更改地址 □	个人投资 □
	支付账单 (如：水电费，话费) □		房屋贷款/个人贷款 □	
	现金取款 □	预定支票本 □	更改密码 □	转账 □
自动化的设备	现金存款 □	账户查询 □	更改地址 □	个人投资 □
	支付账单 (如：水电费，话费) □		房屋贷款/个人贷款 □	

1.14 对于境内/境外的不同消费，请用具体分数 1—5 来表示您选择支付的方式？
(1 表示最少频率使用，5 表示最频繁的使用)

	现金	支票	信用卡	现金卡	网上支付	银行转账
境内	( )	( )	( )	( )	( )	( )
境外	( )	( )	( )	( )	( )	( )

1.15 您的信用卡/现金卡是否具备微型电子芯片和密码功能？ (请在相关项标志)?

信用卡	□
现金卡	□
信用卡和现金卡	□
两者都没有	□

1.16 您是否每月按时缴清信用卡帐单？ 是 □ 否 □ 不一定 □

1.17 请用分数 1—7 表示您对于以下银行业务/产品/商户的信心程度：
(1 表示最低的信心程度，7 表示最高的信心程度)

支票 ( )	网上银行 ( )	自动柜员机 ( )	便利店/加油站 ( )
现金卡 ( )	数据加密 ( )	电子芯片和密码 ( )	购物中心/连锁店 ( )
信用卡 ( )	网上交易 ( )	网上购物 ( )	银行和信用卡公司 ( )

第二节 IT 技能信息

2.1 请选择您使用电脑的频繁程度（工作 / 国家）？(请在相关项标志)

	工作环境		国家环境	
从未使用		□	从未使用	□
非常有限的使用(<1 小时 / 天)		□	非常有限的使用(<1 小时 / 天)	□
偶而几次使用 (1-2 小时 / 天)		□	偶而几次使用 (1-2 小时 / 天)	□
密集性使用 (> 3 小时 / 天)		□	密集性使用 (> 3 小时 / 天)	□

2.2 请选择您尝试过的网上活动 (请在相关项标志)?

网上购物 □　　信息搜索 □　　网上银行 □　　网上交流 □

网上游戏 □　　网上教育 □　　网上下载服务 (例如 音乐 / 视频) □

2.3 迄今为止，您参与各种网上活动的总年数？

网上购物 ____年　　信息搜索 ____年　　网上银行 ____年

网上交流 ____年　　网上游戏 ____年　　网上教育 ____年

网上下载服务 (例如 音乐 / 视频) ___年　　其它（请补充）：_____

2.4 您参与各种网上活动的频率？(请在相关项标志)

	从未使用	每年一次	每季度一次	每月一次	每周一次	每天一次
网上购物	□	□	□	□	□	□
信息搜索	□	□	□	□	□	□
网上银行	□	□	□	□	□	□
网上交流	□	□	□	□	□	□
网上游戏	□	□	□	□	□	□
网上教育	□	□	□	□	□	□
网上下载服务 (例如 音乐 / 视频)	□	□	□	□	□	□

其它（请补充）：_____

2.5 请选择最恰当分数表示您的 IT 技能 (请在相关项标志):

1 = 非常差	2 = 差	3 = 比较差	4 = 普通	5 = 好	6 = 非常好	7 = 优秀
□	□	□	□	□	□	□

2.6 您是否在不同阶段接受过 IT 培训 (请在相关项标志)?

中学	大学	工作	网上课程	自学	职称考核
□	□	□	□	□	□

其它（请补充）：_____

第三节 个人信息

3.1 年龄 (请在相关项标志)

<= 20岁	21-30岁	31-40岁	41-50岁	51-60岁	61-70岁	>71岁
□	□	□	□	□	□	□

3.2 性别 (请在相关项标志)

男性	女性
□	□

3.3 请选择您获得的最高学历？(请在相关项标志)

无正规学历	初中	高中	本科	研究生	不清楚
□	□	□	□	□	□

3.4 您的教育背景是否与 IT 或金融相关 (请在相关项标志)?

IT 相关 □　　金融相关 □　　与 IT 和金融都相关 □　　与两者都不相关 □

3.5 您所经历过金融欺诈*的次数？　　(　　)

*确实发生的欺诈并且产生具体的经济损失。

3.6 您是否经历过企图未遂的金融欺诈？(请在相关项标志)

是 □　　否 □

*虽然有企图进行欺诈，但是没有造成任何经济损失。

3.7 您所遇到企图未遂的欺诈行为的频率？(请在相关项标志)?

	从未使用	每年一次	每季度一次	每月一次	每周一次	每天一次
恶意复制银行卡[1]	□	□	□	□	□	□
身份盗用	□	□	□	□	□	□
垃圾邮件 / 欺诈信函	□	□	□	□	□	□
钓鱼电邮[2] / 欺诈电邮	□	□	□	□	□	□
假冒网站 / 网站劫持[3]	□	□	□	□	□	□
丢失/被盗的银行卡	□	□	□	□	□	□
病毒 / 木马攻击	□	□	□	□	□	□

其它（请举例）：_____

如果您愿意进一步参与此项课题，请提供您方便的联系方式：电话 / 电子邮件 / 邮寄地址：

[1] 恶意复制银行卡是指在银行卡人不知情的情况下擅自非法进行复制。
[2] 钓鱼电邮是指犯罪分子冒充政府机构骗取他人信任和个人银行信息。
[3] 网站劫持指在线用户在毫不知情的状况下被犯罪分子导入到假冒网站并骗取个人信息。

第四节 如果您确实经历过金融欺诈，烦请填写此节内容。

如果您经历过多于一次的欺诈，请自行复印此节。

4.1 在此次金融欺诈中您的总共损失？ 人民币 _____

4.2 此次金融欺诈发生的时间？ 日期: _____月份 _____年度

	8am–1pm (不包含 1pm)	1pm–6pm (不包含 6pm)	6pm–12pm (不包含 12pm)	0am–8am (不包含 8am)
工作日	□	□	□	□
周末	□	□	□	□

4.3 您经历的金融欺诈/ 非法交易所发生的地点 (请在相关项标志)?

工作场所 (例如办公室) □ 公共场所 (例如车站，机场，购物区) □ 家里 □

其它（请补充）：_____

4.4 在欺诈发生后，您在哪一个时间段意识到欺诈行为 (请在相关项标志)?

1— 12 小时 □ 12 — 24 小时 □ 1—7 天 □ 1—2 星期 □ 3—4 星期 □ 长于 1 个月 □

4.5 欺诈行为是如何被发现的 (请在相关项标志)?

核对银行卡账单 □ 信用卡被拒绝接受 □

收到银行的提醒信息 □ 银行卡被拒绝接受 □

收到可疑的物品定购单据 □ 收到莫名其妙的货物 □

其它（请补充）：

4.6 请选择此次金融欺诈的作案手段 (请在相关项标志)?

钓鱼电邮*/欺诈电邮 □ 假冒网站 / 网站劫持* □ 病毒 / 木马攻击 □

丢失/被盗的银行卡 □ 恶意复制银行卡 □ 身份盗用 □

其它（请补充）：_____

*详细解释见前页

4.7 此次欺诈使用了哪种付款方式 (请在相关项标志)?

信用卡 □ 现金卡 □ 预付费卡 □ 支票 □ 网上付款系统 □ 其它（请补充）：

4.8 您是否得到了经济赔偿 (请在相关项标志)?

银行 / 信用卡公司 □　　商家 □　　没有得到赔偿 □　　其它（请补充）：

4.9 为了遏制金融欺诈，您认为谁应该肩负更多的责任 (请在相关项标志)?

银行	信用卡公司	商家	个人 / 用户	警方
□	□	□	□	□

其它（请补充）：

4.10 在经历过欺诈之后，您是否会放弃或者减少相关的网上活动？(请在相关项标志)

	网上银行	网上购物	网上交流	网上游戏
放弃使用	□	□	□	□
减少使用	□	□	□	□
保持原状	□	□	□	□

其它（请补充）：

4.11 您认为普通民众对于金融欺诈的了解程度是什么？(在相关的数字上标志)

更本不了解　　非常清楚的了解

1　2　3　4　5　　了解程度

4.12 对于银行 / 信用卡公司在处理欺诈案件的表现，您的满意程度是？(在相关的数字上标志)

一点都不满意　　非常满意

1　2　3　4　5　　满意程度

4.13 您认为个人银行信息是通过哪个渠道被泄漏的？ (请在相关项标志)

不知道	互联网	邮寄	电话	问卷调查	垃圾桶搜索*	购买物品	自动柜员机
□	□	□	□	□	□	□	□

其它（请补充）：

*i.e. 未销毁的个人信息被犯罪分子从垃圾桶中偷取。

4.14 您认为哪些个人信息可能被非法取得？(请在相关项标志)

名字 □	邮寄地址 □	出身日期 □	电话号码 □
账户号码 □	现金卡号码 □	信用卡号码 □	身份证件号码 □
用户名 / 密码 / 验证码 □		驾驶执照号码 □	电邮地址 □

其它（请补充）：

Bibliography - Section 1: Web References

52xyk.com.cn.***The comparison between Chinese and American credit card slaves*** (http://www.52xyk.com.cn/hangye/shijie/20090210/6176.html ed.). accessed on 22/03/2010

Abbott, B. 23/08/2009. ***Protect against card fraud***. Sunday Express.

American Express, 2010. Fraud Protection Guarantee (https://www212.americanexpress.com/dsmlive/dsm/int/gb/en/personal/membershipbenefits/safesecure/fraudprotection_cm.do?vgnextoid=309f3e37ad444110VgnVCM100000cef4ad94RCRD). accessed on 07/10/2010.

Authorize.Net.***Payment gateway to accept online payments*** (http://www.authorize.net/ ed.). accessed on 22/03/2010

Barclaycard.***Browse credit cards - Barclaycard*** (http://www.barclaycard.co.uk/personal-home/cards/?TC=ASGLA24292&wt.srch=1&mpch=sem ed.). accessed on 14/04/2010

BASE II.***BASE II*** (http://www.answers.com/topic/base-ii ed.)ANSWER.COM. accessed on 22/03/2010

BBC.***Worm affects AOL instant messages*** (http://news.bbc.co.uk/1/hi/technology/4393824.stm ed.). accessed on 25/03/2010

Bekker, S. 2004.

SSL vulnerability affects tens of thousands of sites

(http://redmondmag.com/news/print.asp?EditorialsID=6201 ed.)

RedmondMag.com. accessed on 25/03/2010

CardPaymentInfo.

AVS (address verification system) and CSC/CVV2 (card security code)

(http://www.cardpaymentinfo.co.uk/avs_csc.html ed.). accessed on 22/03/2010

CERN.

The website of the world's first-ever web server (http://info.cern.ch/ ed.).

accessed on 05/03/2007

CFCA.***Internet banking in China growing fast*** (http://server.it168.com/server/2006-12-18/20061218008301.shtml ed.) IT168.com. accessed on 25/03/2010

Charnwood Council.***Charnwood community profile***

(http://www.leics.gov.uk/index/your_council/about_leicestershire/statistics/community_profiles/charnwood_community_profile.htm ed.). accessed on 24/09/2008

CIA.***CIA-the world factbook: United Kingdom***

(https://www.cia.gov/library/publications/the-world-factbook/geos/countrytemplate_uk.html ed.). accessed on 21/03/2007

CNCERT.***About CNCERT/CCC*** (http://www.cert.org.cn/english_web/index.htm ed.).

accessed on 25/03/2010

CNNIC.***Statistics of China internet***

(http://www.cnnic.net.cn/index/0E/00/11/index.htm ed.). accessed on 25/03/2010

CPDRC.***Major statistics of China population 2008***

(http://www.cpirc.org.cn/tjsj/tjsj_cy_detail.asp?id=10410 ed.). accessed on 25/03/2010

Criminal Division,U.S. Department of Justice. ***Internet fraud***

(http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud ed.). accessed on 07/11/2006

Espiner, T. 2009.

Microsoft warns of PowerPoint zero-day flaw (http://news.cnet.com/8301-1009_3-10211443-83.html ed.). accessed on 25/03/2010

Finextra, 2005. Bank of America faces landmark online fraud case,

(http://www.finextra.com/news/fullstory.aspx?newsitemid=13194). accessed on 06/10/2010

Gwade. 17/03/2009.

How we use our credit cards in the UK (http://www.clickcreditcards.co.uk/how-we-use-our-credit-cards-in-the-uk.html ed.).accessed on 04/04/2010

Hong Kong Police Force.***Technology crime statistics in Hong Kong***

(http://www.info.gov.hk/police/hkp-home/english/tcd/overview.htm ed.)Hong Kong Police Force. accessed on 22/01/2007

HSBC.***Personal banking: Banking online HSBC*** (http://www.hsbc.co.uk/1/2/ ed.). accessed on 14/04/2010

Huanqiu.com.***CNCERT released 2007 internet security report*** (http://china.huanqiu.com/focus/2008-04/98011.html ed.). accessed on 28/03/2010

IC3. 2005. ***Internet crime report January 1, 2005 - December 31, 2005***. (http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf:) Internet Crime Complaint Centre. accessed on 06/09/2007

IC3. 2006. ***Internet crime report January 1, 2006 - December 31, 2006***. (http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf:) The Internet Crime Complaint Center. accessed on 06/09/2007

Joris, E.J. 18 Jan 2007. ***T.J. Maxx hack exposes consumer data***. (http://news.cnet.com/T.J.-Maxx-hack-exposes-consumer-data/2100-1029_3-6151017.html) accessed on 25/03/2010

Kranky. ***SSL evasion - growing crisis in online financial transactions*** (http://www.antisource.com/article.php/financial-trans-trojans-ssl ed.). accessed on 05/04/2010

McGlasson, L. 2010. ***37 'Money Mules' Arrested*** Bank information security articles, USA 30/09/2010. (http://www.bankinfosecurity.com/articles.php?art_id=2967) accessed on 06/10/2010

Loughborough University. ***Loughborough university alumni new archive*** (http://alumni.lboro.ac.uk/NetCommunity/Page.aspx?pid=411 ed.). accessed on 05/04/2010

London Evening Standard, 30/03/2007. (http://www.thisislondon.co.uk/news/article-23390837-fraud-victims-told-go-to-the-bank-not-the-police.do). accessed 06/10/2010

Merchant Account Blog. ***Electronic commerce indicator*** (http://www.merchant-account-services.org/blog/electronic-commerce-indicator/ ed.) Merchant Account Blog. accessed on 22/03/2010

Natwest. ***Natwest credit cards*** (http://www.natwest.com/personal/credit-cards.ashx ed.). accessed on 14/04/2010

Natwest Online Banking. Online banking terms and conditions, (http://www.natwest.com/personal/online-banking/g1/legal.ashx) accessed on 14/10/2010.

Nehmzow, C. ***The internet will shake banking's medieval foundations*** (http://www.arraydev.com/commerce/JIBC/9702-01.htm ed.)Booz, Allen and Hamilton. accessed on 10/04/2010

Netease. ***Debit cards farewell to fees free time*** (http://money.163.com/08/1004/10/4NDELFD600252G50.html ed.). accessed on 22/03/2010

NetEase.***Mobile internet users overtake PC internet users in 3 years (china)*** (http://tech.163.com/09/0424/08/57LC21L6000915BE.html ed.). accessed on 22/03/2010

Onyszko, T. ***Secure Socket Layer*** (http://www.windowsecurity.com/articles/Secure_Socket_Layer.html ed.) WindowSecurity.com. accessed on 22/03/2010

People's Bank of China.***Bank cards - an overview*** (http://www.pbc.gov.cn/zhifutixi/zhifugongju/yinhangka/gaishu.asp ed.). accessed on 20/03/2010

Politics.co.uk. 24/08/2007. ***APACS: Online banking usage amongst over 55s*** (http://www.politics.co.uk/press-releases/opinion-former-index/economy-and-finance/apacs-online-banking-usage-amongst-over-55s-$477656.htm ed.). accessed on 11/04/2010

PR China.***China population structure 2009*** (http://www.gov.cn/test/2005-07/26/content_17363.htm ed.). accessed on 11/04/2010

Sohu News. ***Bank card payments into fast growing period*** (http://news.sohu.com/20080619/n257611406.shtml ed.). accessed on 12/04/2010

The UK Cards Association. 2010. ***Card expenditure statistics (CES) - March 2010***. (http://www.theukcardsassociation.org.uk/files/march_2010_commentary.pdf:) . accessed on 02/05/2010

Upmystreet. ***Neighbourhood statistics for Loughborough***

(http://www.upmystreet.com/local/neighbours-in-loughborough.html ed.).

accessed on 22/03/2010

Vanquis. ***Credit card info visa summary - vanquis***

(http://www.vanquis.co.uk/home/Vanquis_Visa_card_summary.aspx ed.).

accessed on 22/03/2010

VISA. a. ***Visa secure commerce***

(http://usa.visa.com/about_visa/press_resources/image_gallery/process_diagrams.html ed.). accessed on 22/03/2010

VISA. b. ***Visa: Process diagrams***

(http://usa.visa.com/about_visa/press_resources/image_gallery/process_diagrams.html ed.)VISA. accessed on 22/03/2010

Visa Integrated Payment Platform.

Visa announces technology milestones

(http://www.paymentsnews.com/2006/09/visa_announces_.html ed.)

PAYMENTS NEWS. accessed on 25/03/2010

Whatis.com.***What is Chip and PIN?***

(http://searchsecurity.techtarget.co.uk/sDefinition/0,,sid180_gci1289642,00.html

ed.). accessed on 22/03/2010

wltzq.gov.cn.***China population characteristics***

(http://www.wltzq.gov.cn/js/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E5%8F%A3%E7%89%B9%E5%BE%81.htm ed.). accessed on 22/03/2010

XinHua News. a. ***China internet users number exceed american*** (http://news.xinhuanet.com/internet/2008-03/14/content_7786806.htm ed.). accessed on 27/03/2010

XinHua News. b. ***Mobile surfers over 100 million in China*** (http://news.xinhuanet.com/internet/2009-02/25/content_10893343.htm ed.). accessed on 27/03/2010

Yang, K., ***The legal issues of credit card service in China, 2010,*** (http://money.sohu.com/20100526/n272354085.shtml). accessed on 14/09/2010

Bibliography - Section 2: Printed Publications

Anderson, R., Bond, M., & Murdoch, S. J. 2006. Chip and spin. ***Computer Security Journal***, 22(2):1-6

APACS. 2006. ***Fraud, the facts 2006***. APACS, The UK Cards Association.

APACS. 2007. ***Fraud, the facts 2007***. APACS, The UK Cards Association.

APACS. 2008. ***Fraud, the fact 2008.*** APACS, The UK Cards Association.

APACS. 2009. ***Fraud, the facts 2009***. APACS, The UK Cards Association.

Baker, C. R. 2002/2. Crime, fraud and deceit on the internet: Is there hyperreality in cyberspace? ***Critical Perspectives on Accounting***, 13(1): 1-15.

Banks move towards two-factor authentication. July 2005. ***Computer Fraud & Security***: page 20.

Barclays' smart approach to online fraud targets 0.5m customers. 2007/4. ***Card Technology Today***, 19(4): 1.

Binational Working Group. October 2006. ***Report on phishing*** Binational Working Group, U.S. Department of Justice.

Black, N.J., Lockett, A., Winklhofer, H. & Ennew, C. 2001. The adoption of internet financial services: A qualitative study. ***International Journal of Retail & Distribution Management***, 29(8): 390--398.

Bryman, A., & Bell, E. 2003. ***Business research methods*** Oxford University Press.

Caunter, N. 2001. The real cost of fraud to E-tailers. ***Computer Fraud & Security***, 2001(8): 17.

Churchill, G.A., & Iacobucci, D. 2002. ***Marketing research: Methodological foundations*** (8th ed.) Harcourt College Publishers.

Consumers losing trust in online banking: Survey. 2007/2. ***Computer Fraud & Security***, 2007(2): 4.

Morse, E.A., & Raval, V. 2008. Security and payment card industry regulation- PCI DSS: Payment card industry data security standards in context. ***Computer Law & Security Report***, 24: 540-554

Field, A. 2009. ***Discovering statistics using SPSS*** (3rd ed.) SAGE Publications Ltd.

Field, A.P. 2000. ***Discovering statistics using SPSS for windows: Advanced techniques for the beginner*** SAGE Publications Ltd.

Furnell, S. & Evangelatos, K. 2007/1. Public awareness and perceptions of biometrics. ***Computer Fraud & Security***, 2007(1): 8-13.

Gengler, B. 2000. Visa and American Express battle credit card fraud. ***Computer Fraud & Security***, 2000(12): 6.

Gerrard, P. and Cunningham, J.B. and Devlin, J.F. 2006. Why consumers are not using internet banking: A qualitative study. ***Journal of Services Marketing***, 20(3): 160-168.

Gralla, P. 2006. ***How personal & internet security works*** Indianapolis, Ind.

Grazioli, S. & Jarvenpaa, S.L. 2000 July. Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. ***IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans***, 30(4): 395-407.

Grazioli, S. 2004. Where did they go wrong? an analysis of the failure of knowledgeable internet consumers to detect deception over the internet. ***Group Decision and Negotiation***, 13(13): 149-172.

Greenemier, L., & Hoover, N. 12 Feb 2007. How does the hacker economy work? ***Information Week***, 1125: 32.

Guo, L. 2008. Risk management of online banking in China: Case study. ***Journal of ABC Wuhan Training College***, 4: 63.

Guo, H.Y. 2004. ***Risk management of online banking in China*** Wu Han University.

Hagel, J., & Brown, J. S. 2001. Your next IT strategy. ***Harvard business review***, 79(9): 105-115.

Harrison, A. 2000. ***Companies point fingers over Nike web site hijacking,*** Computer World, 30 June 2000.

Healey, J.F. 1993. ***Statistics, a tool for social research*** (3rd ed.)Wadsworth Pub. Co.

Howcroft, B., Hamilton, R., & Hewer, P. 2002. Consumer attitude and the usage and adoption of home-based banking in the united kingdom. ***International Journal of Bank Marketing***, 20(3): 111-121.

Holmström B, (1979) Moral Hazard and Observability. ***The Bell Journal of Economics*** 10(1) The Rand Corporation, USA.

Jayawardhena, C. & Foley, P. 2000. Changes in the banking sector - the case of internet banking in the UK. ***Internet Research: Electronic Networking Applications and Policy***, 10(01): 19--30.

Jerving, J. 2007. Fraud from all angles. ***Credit Union Magazine***, 73(6): 30.

Joinson, A. N. 2001. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. ***European Journal of Social Psychology***, 31(2): 177-192.

Kendrick, R.J. 2005. ***Social statistics: An introduction using SPSS for windows, volume 1*** (2nd ed.) Pearson/Allyn and Bacon.

KPMG HK. 2006. ***Fraud and misconduct survey in Hong Kong: 2006 findings***. KPMG Hong Kong.

Lee, H. S., & Kim, S. Y. 2010. Present and future of internet banking in China. ***Journal of Internet Banking and Commerce***, 15(1).

Lei, J. 2002. ***Development strategy of online banks and risk control in China*** University of international business and economics.

Liu, Y. 2008. ***An analysis of bank card in China*** People's University of China.

McGillivray, R.J., & Lieske, S.C. Jul 2001. Webjacking. ***Computer and Internet Lawyer***, 18(7).

McKenna, K.Y.A., Green, A.S., & Gleason, M.E.J. 2002. Relationship formation on the internet: What's the big attraction? ***Journal of Social Issues***, 58(1): 9-31.

Mercado-Kierkegaard, S. 2007. Payments in the Internal Market and the new legal framework-EU law, Harmonising the regulatory regime for cross-border payment services, Computer Law & Security Report, 23:177-187

Muthitacharoen, A.M., Gillenson, M.L., & Suwan, N. 2006/7. Segmenting online customers to manage business resources: A study of the impacts of sales channel strategies on consumer preferences. ***Information & Management***, 43(5): 678-695.

Online retailers in UK lose £580 million to fraud. 2007. ***Computer Fraud & Security***, 2007(6): 3.

Pasquinucci, A. 2007/2. Inside the mind of a spammer. ***Computer Fraud & Security***, 2007(2): 7-8.

Penn, C. 2005. Chip and PIN worldwide. ***HCIMA YEARBOOK 2005***: 34-37.

Pereira, V. 1999. ***Complaint for permanent injunction and other equitable relief*** (Case No.99-1367-A ed.). Federal Trade Commission: United States District Court, Northern District of Florida.

Pitofsky, R. 1998. ***Prepared statement of the federal trade commission on 'internet fraud' before the subcommittee on investigations of the government affairs committee of the united states senate.*** FTC, Washington, DC. Vol. 10, Feb. 1998.

Ratnasingam, P. 2002. The importance of technology trust in web services security. ***Information Management and Computer Security***, 10(5): 255-260.

Ritzer, G. 1995. ***Expressing america: A critique of the global credit card society.*** Pine Forge Press.

Rogers, E. 1962. ***The diffusion of innovation.*** Free Press.

Rotchanakitumnuai, S., & Speece, M. 2003. Barriers to internet banking adoption: A qualitative study among corporate customers in Thailand. ***International Journal of Bank Marketing***, 21(6/7): 312-323.

Shi, H. F. 2009. Card payment and fraud, ***China Court.***

Siegel, S. 1956. ***Nonparametric statistics for the behavioral sciences***. New York: McGraw Hill.

Smith, A.D. 2006. Exploring security and comfort issues associated with online banking. ***Int. J. Electronic Finance***, 1(1): 18-48.

Steennot, R. 2008. Fraudulent payment transactions- Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market. ***Computer Law & Security Report***, 24 : 555-561

Tzenga, Shiang-Feng, Hwangb, Min-Shiang, & Chen, Hsing-Bai. 2005. A secure on-line software transaction scheme. ***Computer Standards & Interfaces***, 27: 303-312.

UK National Statistics. 2008. ***Internet access 2008 - households and individuals***. UK National Statistics Office.

Vance, J. Jun 5, 2006. Guide to two-factor authentication: Factor/ factor. ***Network world***, 23(22): 36.

Walker, I., & Zhu, Y. 2003. ***Education, earnings and productivity: Recent UK evidence***. UK National Statistics Office.

Walker, R.H., & Johnson, L.W. 2006. Why consumers use and do not use technology-enabled services. ***Journal of Services Marketing***, 20(2): 125-135.

Walliman, N., & Baiche, B. (Eds.). 2001. ***Your research project : A step-by-step guide for the first-time researcher*** (2nd ed.)SAGE.

Wang, D. 2007. The development of online banking and future trend in China. ***Finance and Computer***, 1: 8-11.

Wang, Z.X. 2004. ***Introduction to commercial bank in China***. Beijing: China Financial Publishing House.

Whitman, M.E., & Mattord, H.J. 2003. ***Principles of information security*** (3rd ed.). Boston: Mass.

Wilcox, P. 2000. Protecting online merchants from card fraud. ***Computer Fraud & Security***, 2000(9): 4.

Yu, Z. W., & Gong, L. 2004. Analysis of online banking crimes in China. ***Journal of Jiang Su Police Officer College***, 19(5): 176-177.

Zeng, R. 2006. Risk analysis of the internet banking in China, ***China Academic Journal***, 7.

Zhang, Q. 2007. ***Introduction to online banking services in China***. Beijing: China Financial Publishing House.

Zhang, M., & Luo, M. 2009. Fraudulent cases and credit card risk control in China. ***Credit card in China***, 2009:1.