Information & Computer Security

Influential factors of online fraud occurrence in retailing banking sectors from a global prospective: An empirical study of individual customers in the UK and China

Yan Sun Ian Davidson

Influential factors of online fraud occurrence in retailing banking sectors from a global prospective

An empirical study of individual customers in the UK and China

Yan Sun
International Business School Suzhou, Xi'an Jiaotong-Liverpool University, Suzhou P.R. China, and
Ian Davidson
School of Business, Management and Economics, University of Sussex, Brighton, UK

Received 19 October 2013
Revised 13 December 2013
18 February 2014
Accepted 18 February 2014

Abstract

Purpose – This paper aims to focus on online fraud occurrence in retailing banking sectors both in the UK and China. Online financial transactions bring convenience to individuals dramatically and improve banking service quality efficiently. However, the latest service channel, Internet, has been exploited by fraudsters excessively, standing at a huge monetary loss worldwide.

Design/methodology/approach – In aspects of demographic factors, financial activities and IT usage, results would benefit financial organisations and local authorities in strengthening customers' education and improving policymaking. The fraud occurrence model is empirically tested using quantitative data, and comparison is discussed using qualitative data collected in both countries.

Findings – The findings provide solid understanding of customers' behaviours towards online financial transactions and fraud occurrence internationally. As the main implication, customer education is proposed to benefit financial organisations in both countries. According to the data collection process and the data analysis results, individual customers are aware of banking policies and practices to some extent. Particularly in China, customers' satisfaction level is relatively lower and service quality is not reasonable in most circumstances.

Research limitations/implications – The research experiences gained from this study suggest a number of areas for future research, particularly the under-researched area of fraud. Rather than approaching the research questions through individuals, there would be much value in working with merchants and financial organisations that are dealing with financial transactions and fraud on a daily basis.

Originality/value – By combining three approaches (demographic factors, financial activities and IT usage), this study is trying to develop a comprehensive and statistical understanding of online fraud occurrences.

Keywords Consumer marketing, Electronic commerce, Consumer behaviour, Information management, Information security, Computer fraud

Paper type Research paper

Special thanks must go to Loughborough University UK, University of Sussex UK and Xi'an Jiaotong-Liverpool University China.

Information & Computer Security
Vol. 23 No. 1, 2015
pp. 3-19
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-10-2013-0076

1. Introduction

Banks, one type of the financial intermediation organisations, have been playing crucial roles in human society for centuries in Western countries. Retail or personal banking relates to financial services provided to consumers and is usually small-scale in nature (Casu *et al.*, 2006), for instance personal cheque, current accounts, debit/credit cards, mortgage, etc. Supported by the advanced information technology nowadays, modern banks have stepped into our daily life and been serving consumers' demands from various aspects.

Information technology has provided the latest solutions for modern financial industries and transferred the approach to deliver banking service worldwide (Hanafizadeh *et al.*, 2014; Nguyen *et al.*, 2012). However, due to a relatively short history of banks in China, modern financial products and services are brand new concepts for Chinese consumers. Rooted in the biggest emerging market worldwide, financial organisations in China are determined to catch up with international leading players and learn rapidly from their competitors worldwide.

According to a popular article in the *Sunday Express* (Abbott, 2009), more than one in ten of Britain's 20 million online shoppers has either parted with money on a bogus website or knows someone who has. Compared to Western countries, which have been developing financial framework for centuries, the financial industry and organisations in China are at the beginning of their evolution. It is therefore of particular interest to see whether similar issues have started to appear in the Chinese context and how we are going to tackle these problems in both countries.

2. Literature search

Recorded by the People's Bank of China (PBC, 2010), the first bank card was launched in China mainland as a temporary trial in 1979 and the whole process was kept quiet from public. Surprisingly, great change has taken place in the financial market in China within decades. By 2009, the total number of debit cards issued by retailing banks reached 1,180 million, while the sum of credit cards made 187 million (Liu, 2008).

Studied by Worthington *et al.* (2011), early adopters of credit cards in China represent a young and affluent individual group who showed great interests in travelling abroad. Different from their parents' generation, who are used to carrying cash to make payment all the time, the group of young and affluent Chinese embraces the bank card service to avoid inconvenience caused by carrying cash.

Internet, the latest channel of service delivery, even makes payment easier by using bank card details instead of physical cards. Suggested by McKenna *et al.* (2002), four factors were used 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 interaction; and

(4) greater capabilities for social networking.

In other words, customers who are trying to manage their finances on the Internet are attracted mostly by convenience and independence provided by the electronic environment. However, greater anonymity misleads Internet users to believe that they are undoubtedly safe and completely protected on the Internet. Joinson (2001) suggested that computer-mediated communications and general Internet-based behaviour contain high levels of self-disclosure. Nguyen *et al.* (2012) compared online and offline self-disclosure by investigating a number of factors including relationship between communicators, mode of communication and context of the interaction.

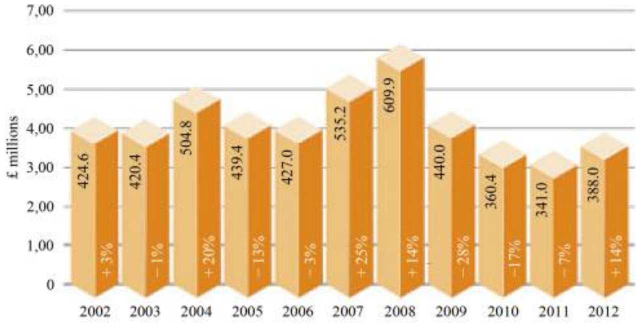
Explained by Grazioli (2004), individuals seek clues of deception by comparing new information with knowledge and experiences they already have. Unfortunately, comparing to the physical world, in which humans have been living for thousands of years, the Internet is still a new and dynamic environment full of uncertainties and challenges for the majority. Furthermore, Logsdon and Patterson (2009) discovered that the Internet is a platform with higher risks for unethical communication and behaviour.

Statistics released by the National Fraud Authority in 2011 show that, fraud loss in the UK has reached £38 billion a year, of which the highest loss occurred in the financial services industry at £3.6 billion (Ash, 2011). As stated in the latest survey conducted by APACS (2013) in 2013, the UK Payment Association, the fraud losses involving the Internet and bank cards have kept increasing in 2012. Figure 1 shows that the loss in the UK alone reached £388.0 million in 2012. This is clearly a very serious problem.

Figure 2 gives an overview of the extent of fraudulent plastic card transactions for UK-issued cards for the period 2002-2012. Fraud losses of each category have had a growth followed by a period of decline as new technologies or procedures have been introduced to combat the fraud. Card-not-present still stays as the fraud type which caused the most loss on UK-issued cards in 2012.

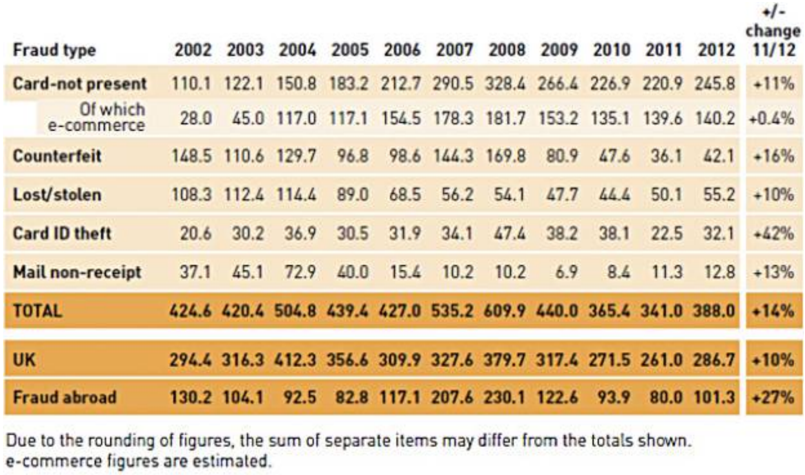
UK is a leading country in adoption of Chip and PIN worldwide. Except for against fraud, there is a liability shift which benefits financial organisations. If a payment is fraudulent, liability for the fraud will go to issuers or acquirers and acquirer will pass the liability back to the merchant, if the merchant is not Chip and PIN-enabled (Penn, 2005). Chip and PIN has been referred to as the biggest change in the means of payment since decimalisation 35 years ago, and several public trials were done in different locations from 1997 to 2003 in the UK (Anderson *et al.*, 2006).

In China today, bank cards are still equipped with magnetic strip and six-digit pin. For any card transaction via POS in China, plastic cards need to be swiped and card holders are requested to enter correct pin to complete the process. Realising the advantages of Chip and PIN system, leading financial organisations in China started



Source: APACS (2013)

Figure 1. Plastic card losses on UK-issued cards 2002-2012



Fraud type	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	+/- change 11/12
Card-not present	110.1	122.1	150.8	183.2	212.7	290.5	328.4	266.4	226.9	220.9	245.8	+11%
Of which e-commerce	28.0	45.0	117.0	117.1	154.5	178.3	181.7	153.2	135.1	139.6	140.2	+0.4%
Counterfeit	148.5	110.6	129.7	96.8	98.6	144.3	169.8	80.9	47.6	36.1	42.1	+16%
Lost/stolen	108.3	112.4	114.4	89.0	68.5	56.2	54.1	47.7	44.4	50.1	55.2	+10%
Card ID theft	20.6	30.2	36.9	30.5	31.9	34.1	47.4	38.2	38.1	22.5	32.1	+42%
Mail non-receipt	37.1	45.1	72.9	40.0	15.4	10.2	10.2	6.9	8.4	11.3	12.8	+13%
TOTAL	424.6	420.4	504.8	439.4	427.0	535.2	609.9	440.0	365.4	341.0	388.0	+14%
UK	294.4	316.3	412.3	356.6	309.9	327.6	379.7	317.4	271.5	261.0	286.7	+10%
Fraud abroad	130.2	104.1	92.5	82.8	117.1	207.6	230.1	122.6	93.9	80.0	101.3	+27%

Due to the rounding of figures, the sum of separate items may differ from the totals shown.
e-commerce figures are estimated.

Source: APACS (2013)

Figure 2.
Losses on UK-issued cards 2002-2012 in relation to fraud type

working on the plan of installation and replacement. Considering customer population and market size, application of Chip and PIN would be time-consuming and labour-intensive in China.

The common way we make online payment in the UK is to submit bank card 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.

In contrast, online shopping in China seems a little complicated because online banking is involved at the start of a transaction. This process does increase the security level for online users. Further solutions to secure online transactions in China vary depending on different financial organisations:

- *One-time PIN generator/digital certificate*: Similar verification scheme has been proposed to mobile banking nowadays and on-time password (OTP) is suggested to work with biometric information to secure fund transfer via mobile devices (Tsai *et al.*, 2012).
- *Instant Text Message confirmation service*: In 2006 (Guo, 2008), the China Construction Bank, one of the big four state-owned banks in China, collaborated with China Mobile and launched an instant financial message service for all customers including account alert, service reminder, transaction confirmation, etc.
- *Virtual keyboard*: It works as the extra protection for customers because virus and Trojans can record characters and numbers typed in using the computer keyboard. Virtual keyboard is generated randomly, which means customers don't follow the same typing route every time.

3. Conceptual background

Theories have been applied into the investigation of innovation adoption for decades. Among the most widely used are technology acceptance model (TAM; Davis, 1989) and innovation diffusion theory (IDT; Rogers, 1995). TAM and IDT have laid a solid foundation and provide the principle approach to study individuals' adoption of technology innovation. However, technology and innovation today have been becoming more and more people-centred and customer-orientated. It is of importance to switch attention from system evaluation itself to users themselves.

So based on TAM and IDT, a few variables including systems usefulness, ease of use and customers' intention were chosen to study individuals' behaviours towards technology innovation, particular the Internet banking service in various countries (Lee, 2009; Celic, 2008; Zhao, 2008). Survey questionnaires were conducted for data collection and data were analysed both quantitatively and qualitatively.

Moreover, demographic factors were added to understand the slow rate of innovation adoption in the UK. Howcroft *et al.* (2002) studied the demographic characteristics of respondents including gender, age, annual income, level of education and ownership of financial products. The result shows that middle age groups (between 35-54 years old) are very likely to adopt Internet banking.

In contrast with the situation in the UK, Worthington *et al.* (2011) studied the credit card usage in the Chinese context, targeting individuals at the average age of 26, who were believed to be early adopters of modern financial products and services in China. The findings suggested that early adopters in China are young, affluent and well-educated who choose cards over cash to make payment.

Besides the demographic research, other studies have focused on customers' attitudes to and behaviour towards the adoption of online financial services. Black *et al.* (2001) once conducted a qualitative study and analysed customers' adoption decisions, in which perceived risk was added to the model as an extra construct to capture the degree of security relative to other banking channels. More recently, Mesiranta *et al.* (2008) and Agarwal *et al.* (2009) suggested that future research trend of Internet banking would focus on customers' perception and users' experiences.

Although potential risks and security issues have been raised in previous studies (Jayawardhena and Foley, 2000; Rotchanakitumnuai and Speece, 2003; Martins *et al.*, 2014; Clemes *et al.*, 2013), not adequate research has been done sufficiently to provide a whole picture and tell a complete story regarding individuals' experience of online financial fraud. Even more obviously, a research gap is whether influential factors of financial fraud exist and how these factors make impacts on fraud occurrence in the electronic environment.

Another line of research into financial transaction and Internet fraud has involved detailed analysis of the computer science and IT technology in areas such as network construction, Internet protocols and data security (Tzenga *et al.*, 2005; Onyszko, 2006). Furthermore, advanced algorisms and encryption models are raised by IT experts to assure that e-transaction/payment is secured (Lin and Hsu, 2011; Vincent *et al.*, 2010).

This category is mainly attracting computer science experts but bringing inspiration to evaluate individuals' IT usage. With the understanding of the characteristics of the Internet and data transmission, this study also covers IT usage of individuals, in particular online activities which might be potential threats to financial transactions in the electronic environment.

By combining three approaches (demographic factors, financial activities and IT usage), this study is trying to develop a comprehensive understanding statistically of the online fraud occurrence. In brief, the conceptual framework of this study is as shown in Figure 3.

4. Research hypothesis

Based on the conceptual model which has been introduced in the previous section, three approaches, demographic factors (Quazi and Talukder, 2011; Lee, 2010), financial activities (Nasri and Charfeddine, 2012) and IT usage (Huang *et al.*, 2011; Davinson and Sillence, 2010), have been applied to investigate fraud occurrences relating to online financial transactions. Research hypotheses and variables are developed in Section 4.1-4.4.

4.1 Demographic factors

Demographic data have been extensively used by business organisations, particularly in retailing sectors in the 1980s (Rogers, 1986; Roweth, 1984). Demographic data are widely used to structure marketing strategies by using descriptions of population subgroups (Pol, 1986). More recently, Powers and Sterling (2008) suggested that relevant demographic indicators can help define segmentation variables in terms of customers' needs and behaviours. Hence, hypotheses with regard to demographic factors are drafted as follows:

H1. Age difference is associated with fraud occurrence on the Internet.

H2. Gender difference is associated with fraud occurrence on the Internet.

H3. Education level difference is associated with fraud occurrence on the Internet.

4.2 Financial activities

Mckechnie (1992) developed an interaction model to study consumer buying behaviours in financial services using long-term buyer–seller relationship. To be more specific, financial activities in this study refer to personal banking usage, such as bank card possession, banking channel usage, account management and service quality. Hence, hypotheses involving financial activities are drafted as follows:

H4. Bank card usage is associated with fraud occurrence on the Internet.

H5. Banking channel usage is associated with fraud occurrence on the Internet.

H6. Account management is associated with fraud occurrence on the Internet.

H7. Customers' satisfaction is associated with fraud occurrence on the Internet.

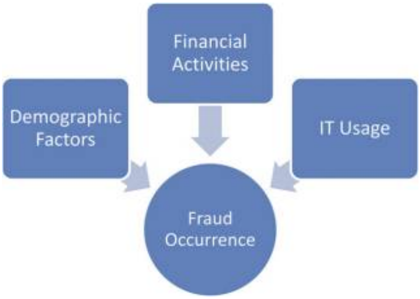


Figure 3.
The conceptual framework

4.3 IT usage

With the dramatic development of network technology, Internet has become a platform for various activities. Beyond the information exploration, data exchange and transmission have been applied by individuals on daily basis. Gralla (2006) studied the vulnerabilities of the electronic environment including Wi-Fi security, browser weaknesses and Trojan/phishing attacks. A few popular online activities are chosen to draft hypotheses regarding individuals' IT usage as follows:

H8. IT skill difference is associated with fraud occurrence on the Internet.

H9. IT usage frequency is associated with fraud occurrence on the Internet.

H10. Online activity is associated with fraud occurrence on the Internet.

5. Research methods and analysis

5.1 Measurement development

Studied by Hoehle *et al.* (2012), survey questionnaire is adopted by researchers to efficiently investigate customer service satisfaction. Most measurement and variables are generated based on previous studies but with an up-to-date touch. Four sections were designed for the questionnaire: personal financial information, IT usage, personal information and fraud case information (optional). The fourth section is optional and exclusive to respondents who have experienced real fraud.

A pre-test survey was carried out to a sample of 200 households in the East-midland area in the UK. In all, 59 replies were received and the responses were analysed carefully for signs of difficulty and ambiguity, and also to gauge whether there might be some omissions. Following this exercise, a few changes were made to the questionnaire in response to comments received.

5.2 Data collection

Following the pilot study, the main survey was carried out in the UK. During two consecutive weekends, 1,200 copies of survey were sent out randomly in a residential area. In the following six weeks, 271 valid replies and 13 partially completed replies were received, giving a response rate of 22.6 per cent. All the replies were examined manually and data were entered into SPSS for analysis. There was no follow-up to non-respondents for ethical clearance purposes. The survey was economised to protect the personal data of the respondents.

In China, we chose a different approach to data collection. 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 northwest area; 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 from the bank's database, most respondents have had experience of using credit/debit cards. A total of 500 questionnaires were sent out and 189 replies were received. Of these, 142 were fully completed, giving a response rate of 28.4 per cent.

5.3 Data analysis

There are two sections of data analysis. We started from demographic data analysis between the UK and China. Then, relevant statistical tests were applied for model building.

5.3.1 Demographic information of respondent in the UK and China. Demographic data were collected in both countries and four variables were selected as follows: age, gender, qualification and education background (IT/finance related). The amount of respondents in the UK is 271 and China is 142. Table I shows an overview of the two data sets.

Seven ranks were used to describe the age distribution of data sets from both countries. It is discovered that UK data spread over all the age ranges, while respondents in China only clustered at four of seven. Supported by interviews with professionals working within the financial industry in China, bank card service is not encouraged to attract consumers who are younger than 20 and older than 60 years. In other words, age group (< 20) represents university and college students in China, while age group (> 60) represents consumers who are retired or near to retirement.

Table I.
Demographic information of respondents in the UK and China

	UK		China	
Variables	Count	(%)	Count	(%)
Age (years)				
< 20	2	0.7	0	0
21-30	22	8.1	74	52.1
31-40	32	11.8	53	37.3
41-50	57	21.0	10	7.0
51-60	48	17.7	5	3.5
61-70	50	18.5	0	0
> 71	60	22.1	0	0
Total	271	100	142	100
Gender				
Male	143	52.8	74	52.1
Female	128	47.2	68	47.9
Total	271	100	142	100
Qualification				
No formal qualification	21	7.7	4	2.8
GCSE/0 level	46	17.0	3	2.1
A level	25	9.2	12	8.5
BSc/BA	111	41.0	92	64.8
Further qualification	58	21.4	29	20.4
Not known	10	3.7	2	1.4
Total	271	100	142	100
IT/Finance-related				
Neither of them	223	82.3	56	39.4
IT-related	18	6.6	9	6.3
Finance-related	23	8.5	61	43.0
Both of them	7	2.6	16	11.3
Total	271	100	142	100
Incidents of actual financial fraud	58	21.4	7	4.9
Total	271		142	

The variable *gender* didn't show much different between two data sets. For the variable *qualification*, two data sets showed a similar distribution and the majority of respondents has received the undergraduate education in both countries.

Interestingly, *education background* (IT/finance related) showed some differences as follows: 82.3 per cent respondents in the UK have an education background neither related to IT nor finance; 43 per cent respondents in the China have an education background related to finance. Comparing to UK, card holders' education background in China is more clustered on finance.

5.3.2 Correlation. SPSS was applied for data analysis and various results are listed in Table II. Ten hypotheses were proposed and different findings were found in two data sets. For the UK data, four of ten hypotheses were statistically significant and accepted, while only one of ten was in China data. Table II shows the correlation and significant value of all hypotheses tested:

H1. Age difference is associated with fraud occurrence on the Internet.

H1 was not supported by the data set collected in both countries. The data showed that the greatest propensity to experiencing fraud is in the 41-50 age group (31.6 per cent) in the UK. In contrast to the age range in the UK data, no respondent in the China survey was aged over 60 years old. In all, 52.1 per cent of the respondents were younger than 31 years old and 37.3 per cent fell into the age group 31-40 years old. 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) people.

H2. Gender difference is associated with fraud occurrence on the Internet.

		UK			China	
Variables	Correlation	Significance value	Hypo	Correlation	Significance value	Hypo
H1	−0.119	0.051	R	0.70	0.406	R
H2	−0.097	0.110	R	0.042	0.618	R
H3	0.105	0.083	R	0.074	0.382	R
H4	−0.022	−0.036	R	0.136	0.116	R
	0.745	0.561		0.100	0.239	
H5	0.211**	0.000	A	−0.055	0.518	R
H6	0.080	0.190	R	−0.019	0.812	R
H7	0.024	0.718	R	0.068	0.432	R
	−0.104	0.090		0.005	0.955	
H8	0.163**	0.007	A	0.046	0.590	R
H9	0.139*	0.023	A	0.040	0.639	R
	0.194**	0.001		−0.058	0.496	
H10	0.212**	0.000	A	0.165*	0.049	A
	0.124*	0.041		−0.048	0.572	R
	0.215**	0.000		−0.058	0.490	
	0.119*	0.050		0.020	0.815	
	0.210**	0.001		0.012	0.889	

Notes: **Correlation is significant at the 0.01 level (two-tailed); *correlation is significant at the 0.05 level (two-tailed); A represents Accepted; R represents Rejected

Table II. Correlation and significance value

Statistical result generated by the UK data set suggests that males are more susceptible to financial fraud than females, almost in the ratio 2:1 (i.e. 62.1 per cent male to 37.9 per cent female). 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 USA. *H2* was not supported by the data set from both countries because the proportion of individuals experiencing fraud is low.

H3. Education level difference is associated with fraud occurrence on the Internet.

Although the highest number of incidences of fraud in the UK was in the BSc/BA/Prof qualification group, this was also the most numerous and the proportions are not significantly different. Undoubtedly, the population in China has a much lower education level than developed countries (wltzq.gov.cn 2004), but the dataset showed that better educated individuals are more likely to access Internet and use bank cards and online banking services in China.

H4. Bank card usage is associated with fraud occurrence on the Internet.

H4 was rejected by statistical results using the data set from both China and the UK, and this finding would be in favour of financial organisations to persuade individuals to adopt online transactions using bank cards.

H5. Banking channel usage is associated with fraud occurrence on the Internet.

Accepted by UK data, *H5* suggests that online banking is the only banking channel that connected with fraud occurrence statistically. Suggested by Dyrud (2006), about 150 British citizens were caught by “419” with a total loss of £8.5 million in 2004, and the UK has made the second place of top ten areas affected by “419” worldwide.

Interestingly, China, the biggest emerging market on earth, was not even mentioned by any previous studies of “419”. Supported by China data of this study, none of the respondents has experienced similar fraudulent scheme so far, and Internet banking channel was not associated with fraud occurrence statistically.

Besides a short history of e-finance services in China, another fact that makes Chinese consumers immune to “419” is the language barrier. Studied by Button (2012), the only country from Asia made on the list of Internet crime origin is Malaysia, in which English is one of the official languages. For individual customers in China, most of them would take an email written in English as a distribution mistake and ignore it without much hesitation.

H6. Account management is associated with fraud occurrence on the Internet.

H6 was rejected by statistical results using the data set from both China and the UK, and this finding would be in favour of financial organisations to persuade individuals to adopt Chip-and-pin function willingly.

H7. Customers’ satisfaction is associated with fraud occurrence on the Internet.

H7 was rejected by statistical results using the data set from both China and the UK, but the data set between two countries suggests different satisfaction levels. In the China data set, five of seven fraud cases (71.4 per cent) 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.

H8. IT skill difference is associated with fraud occurrence on the Internet.

Most instances of fraud in the UK were experienced by the respondents who were confident with their general IT skills (scored average and beyond). 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 overestimate their IT skills. A second possible explanation is that we cannot blame IT technology or IT skills for all fraudulent cases.

Also, many fraudulent cases 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 revealing 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 activities. An interesting fieldwork was conducted in a medium-size IT company in the UK, and financial fraud on the Internet is not a new experience for IT engineers. Most of them have been educated at the university level and hold a degree of computer science.

H8 is not statistically significant in China data. One explanation is that very few fraudulent cases appeared in the data collection in China (7 of 142). But, a similarity showed that majority of the respondents in China scored average and beyond for IT skill evaluation.

H9. IT usage frequency is associated with fraud occurrence on the Internet.

Both data sets from the UK and China showed respondents' confidence with IT skills. *H9* was supported by the UK data indicating that frequent IT users are more likely to be defrauded online. The main explanation comes from browser weakness, which is discussed in the following text.

As the web browser is the working platform for network activities nowadays, it is no surprise that it is a target for fraudsters. Nike.com was webjacked in June 2000, and customers who typed www.nike.com in their web browers were automatically directed to a website in Scotland maintained by a group called S-11and hosted by Firstnet On-line Ltd.

For China data, it didn't show much interesting results regarding *H9* because of smaller data size collected and few fraudulent cases included. However, according to the interviews with industry contacts in China, the banking industry is becoming aware of similar online attacks involving network and browsers. This is emphasised by one of the professionals working in the financial sector. He was working with the IT department within his organisation to set up a separate team dedicated in dealing with online attacks including hardware and software.

H10. Online activity is associated with fraud occurrence on the Internet.

Five various types of online activities were drafted for the survey questionnaire: online shopping, information searching, Internet banking, online communication and downloading media. All the online activities showed a significant relationship with fraud occurrence in the UK data. In contrast, China data only suggested that the usage of online shopping is correlated with fraud occurrence.

The explanation is originated from differences of online payment process in both countries. 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.

The common way we make online payment in the UK and other Western countries 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.

Online shopping in China seems a little more complicated because of the involvement of online banking at the start of the transaction. However, this process does increase the security level for online users. Gradually, online payment process in China is becoming easier if the transaction only involves a small amount of money.

As we learnt from the interviews in China, solutions like One-time PIN/password and Instant Text Message confirmation service have become really popular and successful in protecting customers in both online and offline environments.

5.3.3 Other interesting findings. Besides the correlation and significance values discussed in precious sections, a few more tests were conducted among other variables and are shown in Table III, such as number of credit cards and number of debit cards and satisfaction with credit card service and debit card service. According to the data collected in the UK, we learnt that respondents who have more debit cards are more likely to have credit cards. Similar results came out with the data collected in China.

	UK		China	
Variables	Correlation	Significance value	Correlation	Significance value
Satisfaction with credit card service and history of credit card usage	0.142*	0.035	0.276**	0.001
Number of credit cards & number of debit cards	0.233**	0.000	0.257**	0.002
Satisfaction with credit card service and satisfaction with debit card service	0.623**	0.000	0.367**	0.000
History of branch banking channels usage and history of telephone banking channels usage	−0.055	0.370	0.166*	0.048
Prefer simple password/pin to complicated one and tend to use the same password/pin	0.365**	0.000	0.438**	0.000

Notes: **Correlation is significant at the 0.01 level (two-tailed); *correlation is significant at the 0.05 level (two-tailed)

Table III. Other interesting findings

The reason for the high volume of bank card possession is the current payment policy in China. When a customer applies for a credit card in China, the bank insists that he/she open a currency account; in other words, a debit card would be linked with the credit card to complete the payment process in the future. Due to limited payment methods to pay off credit card in the financial market in China, customers usually take the advice and get a debit card from the same bank, unless he/she would like to bring cash to the counter every month or pay an extra charge monthly using fund transfer between bank accounts.

At the early stage of bank card service, individual customers are still getting used to card usage, while banks are trying to maximise profits by setting extremely high service charges. According to the report by Sina-Finance (2010) in 2010, the development of bank card services has been constrained by service charge rates which are applied to individuals and merchants. Later on, an argument started nationwide by consumers and merchants for reasonable charge rate and appropriate service quality from financial organisations in China.

6. Implications and limitations

6.1 Implications

Online financial transactions bring convenience to individuals dramatically and improve banking service quality efficiently. However, the latest service channel, Internet, has been exploited by fraudsters, standing at a huge monetary loss worldwide (Clemes *et al.*, 2014; Xiao and Bennbasat, 2011; Vishwanath *et al.*, 2011).

The findings provide solid understanding of customers' behaviours towards online financial transactions and fraud occurrence internationally. In aspects of demographic factors, financial activities and IT usage, results would benefit financial organisations and local authorities to strengthen customers' education and improve policymaking in the future.

Also, as a main implication, customer education is proposed to benefit financial organisations in both countries. According to data collection process and data analysis results, individual customers are aware of banking policies and practices to some extent. Particularly in China, customers' satisfaction level is relatively lower and service quality is not reasonable in most circumstances.

To combat online financial fraud via customer education, two approaches are suggested: to reduce online self-disclosure and to detect online deception. Firstly, awareness of online self-disclosure is the first step to understand customers' behaviours on the Internet and the link between individuals' attitude and behaviours can be established successfully (Joinson *et al.*, 2010; Schiffrin *et al.*, 2010; Taddei and Contena, 2013). Secondly, it is important to help customers receive sufficient information and materials on detecting online deceptions, which are actually old tricks but disguised by new channel – Internet (Wright *et al.*, 2010; Mavlanova and Fich, 2010).

6.2 Limitations

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 organisations that are dealing with financial transactions and fraud on a daily basis.

If a researcher could get around this veil of secrecy, there would be much interesting information and data to analyse. It is hoped that the author of this article 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.

Also, M-commerce including M-shopping and payment started to develop rapidly worldwide (Mallat, 2007). It would be interesting to investigate whether customers' attitude and behaviours in e-environment are different from when in m-environment.

References

Abbott, B. (2009), "Protect against card fraud", *Sunday Express*, 23 August.

Agarwal, R., Rastogi, S. and Mehrotra, A. (2009), "Customers' perspectives regarding e-banking in an emerging economy", *Journal of Retailing and Consumer Services*, Vol. 16 No. 5, pp. 340-351.

Anderson, R., Bond, M. and Murdoch, S.J. (2006), "Chip and spin", *Computer Security Journal*, Vol. 22 No. 2.

APACS (2013), *Fraud, the Facts 2013*, APACS, The UK Cards Association, London.

Ash, D. (2011), "The UK fraud landscape for financial services", *Computer Fraud & Security*, Vol. 2011 No. 4, pp. 16-18.

Black, N.J., Lockett, A., Winklhofer, H. and Ennew, C. (2001), "The adoption of Internet financial services: a qualitative study", *International Journal of Retail & Distribution Management*, Vol. 29 No. 8, pp. 390-398.

Button, M. (2012), "Cross-border fraud and the case for an 'interfraud'", *An International Journal of Police Strategies & Management*, Vol. 35 No. 2, pp. 285-303.

Casu, B., Girardone, C. and Molyneux, P. (2006), *Introduction to Banking*, Pearson, Prentice Hall, Edinburgh.

Celic, H. (2008), "What determines Turkish customer's acceptance of Internet banking?", *International Journal of Bank Marketing*, Vol. 26 No. 5, pp. 353-370.

Clemes, M.D., Gan, C. and Zhang, J.L. (2013), "An empirical analysis of online shopping adoption in Beijing, China", *Journal of Retailing and Consumer Services* (in press).

Clemes, M.D., Gan, C. and Zhang, J.L. (2014), "An empirical analysis of online shopping adoption in Beijing, China", *Journal of Retailing and Consumer Services*, Vol. 21 No. 3, pp. 364-375.

Davinson, N. and Sillence, E. (2010), "It wont's happen to me: promoting secure behaviour among Internet users", *Computers in Human Behavior*, Vol. 26 No. 6, pp. 1739-1747.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use and user of acceptance of information technology", *MIS Quarterly*, Vol. 3 No. 3, pp. 319-340.

Dyrud, M. (2006), "I brought you good news. An analysis of Nigerian 419 letters", *Proceedings of the 2005 Association of Business Communication Annual Convention, Irvine, CA*.

Gralla, P. (2006), *How Personal & Internet Security Works*, QUE, Indianapolis, IN, p. 91.

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*, Vol. 13 No. 13, pp. 149-172.

Guo, L. (2008), "Risk management of online banking in China: case study", *Journal of ABC Wuhan Training College*, Vol. 4, p. 63.

Hanafizadeh, P., Keating, B.W. and Khedmatgozar, H.R. (2014), "A systematic review of Internet banking adoption", *Telematics and Informatics*, Vol. 31 No. 3, pp. 492-510.

Hoehle, H., Scornavacca, E. and Huff, S. (2012), "Three decades of research on consumer adoption and utilization of electronic banking channels: a literature analysis", *Decision Support Systems*, Vol. 54 No. 1, pp. 122-132.

Howcroft, B., Hamilton, R. and Hewer, P. (2002), "Consumer attitude and the usage and adoption of home-based banking in the United Kingdom", *International Journal of Bank Marketing*, Vol. 20 No. 3, pp. 111-121.

Huang, D.-L., Rau, P.-L.P., Salvendy, G., Gao, F. and Zhou, J. (2011), "Factors affecting perception of information security and their impacts on IT adoption and security practices", *International Journal of Human-Computer Studies*, Vol. 69 No. 12, pp. 870-883.

Jayawardhena, C. and Foley, P. (2000), "Changes in the banking sector - the case of Internet banking in the UK", *Internet Research: Electronic Networking Applications and Policy*, Vol. 10 No. 1, pp. 19-30.

Joinson, A.N. (2001), "Self-disclosure in computer-mediated communication: the role of self-awareness and visual anonymity", *European Journal of Social Psychology*, Vol. 31 No. 2, pp. 177-192.

Joinson, A.N., Reips, U.D., Buchanan, T. and Schofield, C.B.P. (2010), "Privacy, trust and self-disclosure online", *Human-computer Interaction*, Vol. 25 No. 1, pp. 1-24.

Lee, M.C. (2009), "Factors influencing the adoption of Internet banking: an integration of TAM and TPB with perceived risk and perceived benefit", *Electronic Commerce Research and Applications*, Vol. 8 No. 3, pp. 130-141.

Lee, J.-W. (2010), "The roles of demographics on the perceptions of electronic commerce adoption", *Academy of Marketing Studies Journal*, Vol. 14 No. 1.

Lin, H.-Y. and Hsu, C.-L. (2011), "A novel identity-based key-insulated convertible authenticated encryption scheme", *International Journal of Foundations of Computer Science*, Vol. 22 No. 3, pp. 739-756.

Liu, Y. (2008), "An analysis of bank card in China", MSc dissertation, People's University of China, Beijing.

Logsdon, J.M. and Patterson, K.D.W. (2009), "Deception in business networks: is it easier to lie online?", *Journal of Business Ethics*, Vol. 90 No. 4, pp. 537-549.

Mckechnie, S. (1992), "Consumer buying behaviour in financial services: an overview", *International Journal of Bank Marketing*, Vol. 10 No. 5, pp. 4-12.

McKenna, G., McKenna, K.Y.A., Green, A.S. and Gleason, M.E.J. (2002), "Relationship formation on the Internet: what's the big attraction?", *Journal of Social Issues*, Vol. 58 No. 1, pp. 9-31.

Mallat, N. (2007), "Exploring consumer adoption of mobile payments – a qualitative study", *Journal of Strategic Information Systems*, Vol. 16 No. 4, pp. 413-432.

Martins, C., Oliveira, T. and Popovic, A. (2014), "Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application", *International Journal of Information Management*, Vol. 34 No. 1, pp. 1-13.

Mavlanova, T. and Fich, R.B. (2010), "Counterfeit products on the Internet: the role of seller-level and product-level information", *International Journal of Electronic Commerce*, Vol. 15 No. 2, pp. 79-104.

Mesiranta, N., Maenpaa, K., Kale, S.H. and Kuusela, H. (2008), "Consumer perceptions of Internet banking in Finland: the moderating role of familiarity", *Journal of Retailing and Consumer Services*, Vol. 15 No. 4, pp. 266-276.

Nasri, W. and Charfeddine, L. (2012), "Factors affecting the adoption of Internet banking in Tunisia: an integration theory of acceptance model and theory of planned behavior", *Journal of High Technology Management Research*, Vol. 23 No. 1, pp. 1-14.

Nguyen, M., Bin, Y.S. and Campell, A. (2012), "Comparing online and offline self-disclosure: a systematic review", *Cyberpsychology, Behavior and Social Networking*, Vol. 15 No. 2.

Onyszko, T. (2006), "Secure socket layer", WindowSecurity, available at: www.windowsecurity.com/articles/Secure_Socket_Layer.html (accessed 22 March 2010).

Penn, C. (2005), "Chip and PIN worldwide", *HCIMA YEARBOOK*, pp. 34-37.

PBC (2010), "People's Bank of China. Bank cards – an overview", available at: www.pbc.gov.cn/zhifutixi/zhifugongju/yinhangka/gaishu.asp (accessed 20 March 2010).

Pol, L.G. (1986), "Marketing and the demographic perspective", *The journal of Consumer Marketing*, Vol. 3 No. 1, pp. 57-65.

Powers, T.L. and Sterling, J.U. (2008), "Segmenting business-to-business markets: a micro-macro linking methodology", *Journal of Business & Industrial Marketing*, Vol. 23 No. 3, pp. 170-177.

Quazi, A. and Talukder, M. (2011), "Demographic determinants of adoption of technological innovation", *Journal of Computer Information Systems*, Vol. 51 No. 3.

Rogers, D. (1986), "Demographic data reports", *Retail & Distribution Management*, Vol. 14 No. 5, pp. 23-26.

Rogers, E.M. (1995), *Diffusion of Innovations*, 4th ed., Free Press, New York, NY.

Rotchanakitumnuai, S. and Speece, M. (2003), "Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand", *International Journal of Bank Marketing*, Vol. 21 Nos 6/7, pp. 312-323.

Roweth, B. (1984), "Sources of data: demographic/educational/social", *Aslib Proceedings*, Vol. 36 Nos 11/12, pp. 429-435.

Schiffrin, H., Edelman, A., Falkenstern, M. and Steward, C. (2010), "The associations among computer-mediated communication, relationships and well-being", *Cyberpsychology, Behavior and Social Networking*, Vol. 13 No. 3.

Sina-Finance (2010), available at: http://finance.sina.com.cn/money/bank/bank_hydt/20110304/07109470268.shtml (accessed 2 July 2013).

Taddei, S. and Contena, B. (2013), "Privacy, trust and control: which relationships with online self-disclosure?", *Computer in Human Behavior*, Vol. 29 No. 3, pp. 821-826.

Tsai, C.L., Chen, C.J. and Zhuang, D.J. (2012), "Secure OTP and biometric verification scheme for mobile banking", *2012 Third FTRA International Conference on Mobile*, *Vancouver*, Ubiquitous and Intelligent Computer.

Tzenga, S.-F., Hwangb, M.-S. and Chen, H.-B. (2005), "A secure on-line software transaction scheme", *Computer Standards & Interfaces*, Vol. 27, 303-312.

Vincent, O.R., Folorunso, O. and Akinde, A.D. (2010), "Improving e-payment security using Elliptic Curve Cryptosystem", *Electronic Commerce Research*, Vol. 10 No. 1, pp. 27-41.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011), "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model", *Decision Support Systems*, Vol. 51 No. 3, pp. 576-586.

Wang, D. (2007), “The development of online banking and future trend in China”, *Finance and Computer*, Vol. 1, pp. 8-11.

Worthington, S., Thompson, F.M. and Stewart, D.B. (2011), “Credit cards in a Chinese cultural context – the young, affluent Chinese as early adopters”, *Journal of Retailing and Consumer Services*, Vol. 18 No. 6.

Wright, R., Chakraborty, S., Basoglu, A. and Marett, K. (2010), “Where did they go right? Understanding the deception in phishing communications”, *Group Decision and Negotiation*, Vol. 19 No. 4, pp. 391-416.

Xiao, B. and Bennasat, I. (2011), “Product-related deception in e-commerce: a theoretical perspective”, *MIS Quarterly*, Vol. 35 No. 1 pp. 169-195.

Zhao, A.L. (2008), “Perceived risk and Chinese consumers’ Internet banking services adoption”, *International Journal of Bank Marketing*, Vol. 26 No. 7, pp. 505-525.

Further reading

Harrison, A. (2000), “Companies point fingers over Nike web site hijacking”, *Computer World*, 30 June.

Hoehle, H., Scornavacca, E. and Huff, S. (2012), “Three decades of research on consumer adoption and utilization of electronic banking channels: a literature analysis”, *Decision Support Systems*, Vol. 54 No. 1, pp. 122-132.

McGillivray, R.J. and Lieske, S.C. (2001), “Webjacking”, *Computer and Internet Lawyer*, Vol. 18 No. 7.

Pereira, V. (1999), “Complaint for permanent injunction and other equitable relief”, Case No. 99-1367-A, 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”, Vol. 10, FTC, Washington, DC.

Salu, A.O. (2004), “Online crimes and advance fee fraud in Nigeria- are available legal remedies adequate?”, *Journal of Money Laundering Control*, Vol. 8 No. 2, pp. 159-167.

Zhang, Y., Fang, Y., Wei, K.-K., Ramsey, E., McCole, P. and Chen, H. (2011), “Repurchase intention in B2C e-commerce - a relationship quality perspective”, *Information & Management*, Vol. 48 No. 6, pp. 192-200.

Corresponding author

Yan Sun can be contacted at: YAN.SUN@xjtlu.edu.cn