Fraud Responses through Short Text Messages (SMS): A Qualitative Study on Enthusiasm, Power of Influences and Impactsto the University Students

Mohamad Ridhuan Mat Dangi
Norulhuda Tajuddin

ABSTRACT

The rapid growth of technology especially in the telecommunication field today brings the pro and contra upon its implementation. The digital waves have transformed the communication process among people around the world. The Short Text Message Service or SMS for short is one of the features contained in the mobile phone that is popularly used by the users. Despite being meaningful to ease users communicating with others remotely and globally, it also brings together the chances and opportunities for the criminal actions. Among the well-known criminal activities related to the use of SMS is the fraud SMS; operatingin different types of conduct. The fraud activities also evolve from time to time in line with the development of technologies that allows the fraudster to creatively manipulate the SMS services as a trap to the victims.Therefore, this study is conducted with the objectives to discover factors which motivate an individual to respond to fraud SMS, to identify the reasons why victims are susceptible to fraud SMS, to recognize the impacts received by individuals who are victims of fraud SMS and to identify and determine the appropriate measures to avoid and prevent the problem of fraud SMS. This study revealed that, one can receive 1 to 5 fraud SMSes since they have started using mobile phones. A majority of the respondents are aware of the fraud SMS and agree that it is a form of cheating through mobile technology. The individual's attitude, behavior and financial problems are among the reasons why the victims response to fraud SMS.

Keywords: *fraud, fraud SMS, spam*

Introduction

The rapid growth of technology nowadays has shaped the human life in modern society. Many aspects of activities such as work, daily routines, recreation, communication and others receive the impact from the development of technology globally. Indeed the involvement in the element of technology can make our lives easier and simpler in doing tasks or personal activities. In the case of communication, people now can communicate with others at anytime and anywhere regardless of any boundaries with the aid of high-tech communication channel and devices. People can no longer have a face-to-face conversation in order to communicate or exchange of opinion since the existence of internet technology which has enable this process to be conducted just with a tip of the finger. Despite the usefulness of technology in our lives, it also can become an ideal medium for the criminals especially the fraudster to perform their illegal activities to trick others. Fraud can be perpetrated by anyone and it can exist in a variety of forms (El Tawashi, 2010). One example of fraud infecting the telecommunication services is the fraud SMS.

SMS or the Short Messaging Serviceis the service provided by the telecommunication provider which allows people to send text messages over to others through mobile phones. This service supports the function of sending and receiving alphanumeric text which can ease the users to communicate other than using the voice call function. With nowadays advanced technology, the mobile phone providers have come out with interesting features for their devices and the application software. With these features, sending messages and communicating through SMS becomes fun and enjoyable.Nowadays, the SMS services are not only applicable for sending and receiving text messages, but it also has gone forward with a variety of services such as mobile transactions, news, advertisements and entertainment activities. Some of the service providers in certain countries use SMS as a medium to disseminate information. For example, as reported by Maharani et al. (2012), there is an initiative taken by several NGOs to spread information about healthcare and medicines to the consumers. Some countries, such as Nigeria, SMS service is used to deliver information about e-government and its services to the citizens, business entity and also the government institution. There

are some reasons why the SMS service is chosen as their initiative to deliver such information and services. According to Chete et al. (2012), the logical approach for delivering such services through SMS is mainly because of the huge number of SMS users, extensive infrastructure of SMS and the cost is much lower than the internet.

However, fraudsters can manipulate this service and make it as a medium to commit fraud activities with deceitful intentionsof thefts and causing losses.There are many cases reported and published in the media regarding fraud SMSes. For example, Subex Telecom Fraud Alerts (2012) reported a case in Indonesia where a senior executive of a telecom operator is being questioned on suspicions of participating in a premium rate SMS scam resulted in criminals getting away with $1.3million per month. Meanwhile a case in France shows that two men were arrested for a suspicion of developing mobile malware and scams which conned out from each user in an average of 20 Euro or 30 Euro and managed to collect almost 100,000 Euro. These cases have shown that the fraud activities are a serious problem and with the potential of causing a huge amount of losses suffered by not only the service providers but also to its customers overall. Since the numbers of SMS users are huge and this service isused worldwide, the chances of victims of fraud SMS could be reasonably high. Therefore, an initiative must be carried out to educate users on how appropriate responses and actions towards fraud SMS can be taken.

Literature Review

In general, fraud is defined as the action that involves intentional deception whether by error or deliberate error to cause the victims to suffer the losses or damages (Kranacher et al.,2011). The fraudulent activities can be committed by anyone and can be in various methods and techniques used by the perpetrators. Meanwhile the fraud SMS is one of the stems in telecommunication fraud that can be definedas any action involves the theft of services or deliberate abuse of voice and data networks to cause losses to the victims or avoid any charges by the service provider (Brown, 2005). In relation with fraud triangle theory developed by Cressey, the fraud perpetrators are motivated to commit such activities driven by the elements of opportunity, pressure and rationalization. In the view of victims of the fraud SMS, the question arises: why they areresponding towards the fraud SMS. By looking into one of the elements in the fraud triangle theory which is the pressure, it is assumed that the victim of fraud SMS could also feel the pressures that drive them in response to the SMS. For example, a user who face financial pressure and suddenly receives the message of winning of cash prizes in a contest would reasonably reply that message although it requires some personal or other relevant information.

According to Puukangas et al. (2010) in his study, among the types of fraudulent SMS are spoofing, spamming, faking, flooding, Global Title (GT) Scanning and mobile malware. According to this author, the SMS spam is a common problem in the countries of Asia and the U.S.A. The spam message usually can contain commercial information, bogus contest and includes the intention to invite responses from the receiver (Puukangas et al. 2010). For example, some users have experienced a situation whereby they receive the SMS from certain parties claiming themselves as the corporate or business entity announce the user as the winner which they never participate. If the user is not careful, they will be easily deceived and tricked which will lead them to give their personal information such as bank account, identification number and so forth without realizing that they have become victims of the fraud syndicate that uses SMS as a medium.

The SMS flooding is resulted from multiple spam SMS posed by multiple subscribers to a single destination resulted to the overloading of SMS and slow down the network (Buehler, 2004). The SMS spoofing and faking are usually caused by a third party who want to pressure and let down the targeted service provider by causing its customer to feel dissatisfied upon the slow network from the overload of fake SMS. It also can createwrong interconnection billing, wrong address of delivering SMSand also cancontribute to the SMS flooding. Dissatisfied customers will then try to terminate their services with the attacked service provider. As a consequence, the targeted service provider will receive losses from reducing the revenues, damage reputation and loss of customer's trust. As for the case of GT scanning, the fraudsters attempt to find the weakest point in the network system of the SMS service. The fraudster will try to find unprotected systemin the SMS center by scanning of the network and taking control the SMS system. This type of fraud SMS usually requires the fraudster to use mobile phone with a computer connection in order to perform this activity.

The emergence of mobile business and mobile banking are able to increase the risk of fraud to occur in the telecommunication services via SMS. Many financial institutions have put their trust on service providers and cooperate together in performing the mobile banking and many services or transactions that can be made through mobile phones. According to Murynets and Jover (2012), a study conducted by AT&T on spam analysis found out that mobile spam is increasing and grows by 500% yearly mainly because of the unlimited messaging plan and widespread of mobile internet technology. The result also highlighted that 99.64% of the spammers use pre-paid accounts with the average period of 7 – 11 days of active illegitimate account. This shows that, the perpetrators will always change their mobile phone account to conceal their activity and avoid being arrested.

The advancement of internet technology and a state of the art device make people around the globe employ such technology in their communication and social networking to keep in touch with friends, families or business purposes. According to the survey of International Telecommunications Union (ITU) in 2005, there are now over six billion global mobile subscribers for an average global penetration rate of 87% making SMS the primary service on mobile devices with an average of 200,000 SMS were sent in every second (Cloudmark, 2012). This fact gives the picture that there is a high opportunity for the fraudsters to conduct their activities with a lot of potential victims waiting. Thus, there is a need for continuous research and active investigation is required to counter the fraud SMS from being overwhelmed. With the increasing case of fraud SMS, it will cause the users unable to identify which of the SMS they receive is either valid or invalid. Thus, there must be an action plan to keep the pace of advancement in the telecommunication and the internet technology in line with the promises security to reduce the risk of fraud and other potential threats using mobile phone.

In Malaysia, fraud SMS has been widely spread to many mobile phone users, involving well-known business entity activities such as Shell, Power Root, Astro, Digi, or Petronas and etc. Fraudsters disguise over this well established organization to deceive users since it is already trusted by customers. Therefore, numerous companies and financial institution have taken step to provide the notice and some other initiative to let their customers become aware of the fraud SMS and scams which are using their names. For example, the Poslaju Malaysia has presented the important noticeprovided in two-language version of Bahasa Malaysia and English (Figure 1 and Figure 2) at their counter and notice board to advise customers to be aware of fraud activities through emails or SMS asking for personal information or money. The Central Bank of Malaysia also provides notice and announcement on their official website to alert public about the fraudulent calls, emails and SMS requesting for personal banking information. Other financial institution such as Affin bank and Bank Simpanan Nasional (BSN) also provide the notice and announcement on their websites regarding the same issues. On the other hand, Bank Islam Malaysia Berhad (BIMB) provides the notice of fraud activities that appear on the screen of Automated Teller Machine (ATM) provided in every branch in order to alert their customers about fraud SMS. Table 1 below shows examples of fraud SMS using some of well-known companies as received by users.For privacy and security purposes, the phone number and name in the example of fraud SMS were not exposed.

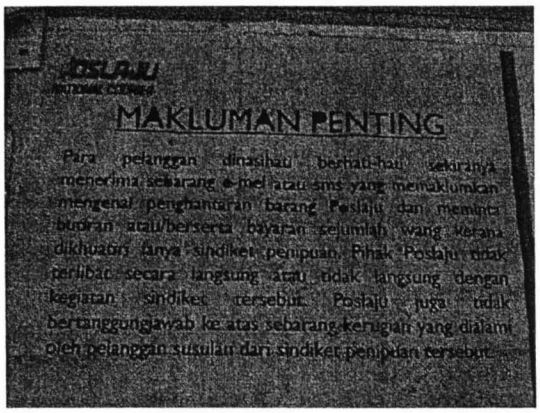

Figure 1: Malay version of fraud alert from Poslaju Malaysia

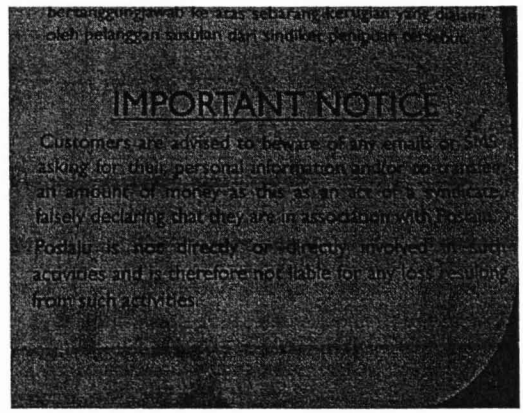

Figure 2: English version of fraud alert from Poslaju Malaysia

Table 1: Example of fraud SMS disguised as well established companies

Companies	Types of SMS sent to the targeted mobile phone number
Shell	"You winner!!! You won a lucky draw of RM30, 000 from SHELL 9013445 SERIAL NO 8xxxxx, call the office: +62xxxxxxxx :From: Mr. xxxxxxx"
Power Root	CONGRATULATIONS! YOUR SIM CARD HAS WON RM 10,000 from POWER ROOT-Serial No. F2E57C. For info..call; Mr. xxxxxxx at 014-xxxxxxx
Astro	"Congratulations...Your simcards win cash checks of 5000 from Akademi Fantasia Malaysia (AFM) l. Please contact 006xxxxxxxxx/0062xxxxxxxxxx1. "
Digi	"Congratulations! You have won a CASH PRIZE worth RM7,000 from DiGi. Please call DiGi Customer Service at 006xxxxxxxxxx." "Forward from +601xxxxxxxx.. this is DiGi special gift for every DiGi user. Just send this message to another 10 DiGi user and you'll get RM50 free automatic."
Petronas	"Congratulations! Your SIM Card Have Win Lucky Bonus Checks of RM15, 000 from PETRONAS, Please Call In Line 006xxxxxxxxxxx Thank you. "

Source: Irwan Dahnil and Salleh Esa (2008)

Research Methodology

This qualitative study employed a phenomenological research methodology as it is concerned with the study of experience from the perspective of the individual (Stan Lester, 1999). Other than that, this study has been conducted in qualitative method since the exploratory nature of this study is the best approach for the researchers to obtain data in more detail and wider perspective (Creswell, 2003). Strauss and Corbin (1998) mentioned that, qualitative approach enables researchers to obtain data that are more detailed which involves one's perceptions, feelings and thinking with regard to a particular phenomenon. According to Creswell (2003), the sample set in qualitative research tends to be relatively small and can range from 1 or 2 to 30 or 40 participants. In this study, the respondents are 20 Diploma students from various faculties such as Accountancy, Plantation and Agrotechnology, and Business Management. This study uses a purposive sampling where the students who have experiencedreceiving and respond to fraud SMS are selected to become the participants in live interviews conducted by the researchers. Hence, this sampling method allows researchers to gain a deeper understanding towards the issue through the interview process. The open ended semi-structured interview questions were designedto explore or discover new knowledge framed by the main research questions as follows:

a) To discover factors which motivate an individual to respond to fraud SMS.
b) To identify the reasons why victims are susceptible to fraud SMS
c) To recognize the impacts received by individuals who are victims of fraud SMS
d) To identify and determine the appropriate measures to avoid and prevent the problem of fraud SMS.

The interview questions are divided into two parts. Part A asked about the participant's information while Part B contains questions about the fraudulent SMS in terms of their knowledge, experience, frequency in receiving fraud SMS, level of awareness, motivation to response fraud SMS, power of influences, impacts, step to avoid and preventive action methods. This study uses semi-structured, recorded, transcribed interviews in order to explore the perceptions of the participants. Before the interview session begins, the participants are given a short time (15 minutes to 20 minutes) to review the questions to allow them to get ready for the interview process. Field data were collected by the researchers at site conducive to anonymity, relatively quiet for recording purposes and free from interruptions. There are several techniques and a procedure provided in many previous literatures provide strategies to check the accuracy and findings for the qualitative researchers (Creswell, 2003; Morse et al. 2002; Tuckett, 2005).

For this study, the researchers use different data source to triangulate the findings; make use of rich, thick descriptions to convey the findings, clarify any bias, and keep field notes of each interview. The

researchers recorded the interview sessions using two types of digital devices namely Samsung audio recorder and Blackberry audio recorder and the audio files were kept in the hard disk for storage and retrieval purposes.For the data analysis, the researcher used Nvivo Version 10 for the transcribing process to convert the audio format data into text form. The same software is also used in order to create the verbatim transcript for each word mentioned by the participants inthe coding process. Researchers also validate the accuracy of the verbatim transcripts by listening to each recorded interview and compared it to the written transcripts.

The words which contain substantial information related to the study are included in the theme for the next data analysis. In order to increase the reliability of the study, the researchers used several methods such as writing thick, rich detailed systematic descriptions of the procedures taken, explain the findings in detail, create field notes and provide detailed description of the contextual setting for each interview. The researchers also use two voice-activated digital recorders and use the combination of voice transcription software and personal validation in creating the verbatim transcripts.

Results and Findings

This part comprises of four sections of analysis which is demographic of respondents, experience and awareness in receiving fraudulent SMS, fraudulent SMS, and fraud SMS avoidance and prevention method from respondent's perspectives. Since this is a qualitative study, the themes or key phrases were based on researcher's best judgement, and used validity and reliability techniques.

i) Demographic of respondent

Demographic data were captured from research participant as part of the data collection process. Names were kept confidential. The data presented in the tables uses capital R followed by number to represent the respondents. The numbering systemallows one to identify, which research participant provided the information while maintaining confidentiality.

The demographic table (Table 2) summarizes the gender, age, program enrolled, source of finance and average family income. Based on the table, there were 12 male respondents and another 8 are female. Eleven of them are aged between 18 to 20 years old and 9 respondents were aged between 20 to 23 years old. The respondents were enrolled in 4 diploma programmes; 6 respondents enrolled in Diploma in Banking and Diploma in Accountancy, respectively. Meanwhile, 4 respondents have enrolled in Diploma in Business and there were also 4 respondents enrolled in Diploma in Plantation and Agrotechnology.

The respondents were asked regarding their source of finance for their study. 9 respondents were recorded to receive an education loan from Perbadanan Tabung Pendidikan Tinggi Nasional (PTPTN). There were 7 respondents who received financial assistance from their parents. 2 were reported to have both PTPTN and self funded and another 2 have received from other sources of financing such as bank scholarship and PERKESO. Next, the respondents were asked about the average family income. 11 respondents have reported their family receive more than RM2,001 per month. 3 respondents reported to receive between RM1,501 to RM2,000, and 2 respondents get RM0 to RM500, 2 respondents get RM501 to RM1,000 and 2 respondents get between RM1,001 to RM1,500.

Table 2: Demographic result

Demographic category		**N**	**Percent %**
Gender	Male	12	60
	Female	8	40
Age	18 yearsto 20 years	11	55
	20 years to 23 years	9	45
Program	Diploma in Banking	6	30
	Diploma in Business	4	20
	Diploma in Accountancy	6	30
	Diploma in Plantation and Agrotechnology	4	20
	PTPTN	9	45

Source of finance	Self funded	7	35
	Both, PTPTN and self funded	2	10
	Other	2	10
Average family income (RM)	0 – 500	2	10
	501 – 1,000	2	10
	1,001 – 1,500	2	10
	1,501 – 2,000	3	15
	More than 2,001	11	55

Table 3 summarized the experience of receiving any SMS stated the respondents won any competition or any activities that they have never involved. All 20 respondents have received this kind of SMS. It shows, this fraud SMS case can be considered as a big issue to highlight and the selection sample of respondents also are related to this study.

ii) Experience in receiving fraudulent SMS

Table3: Experience received fraud SMS by respondent

Have you receive any SMS stated you have won any competition or any activities that you never know about it?	**N**	**Respondent**
Yes	20	R1, R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R20
No	0	

Next, the respondents were also asked regarding frequency to receive the SMS. 16 respondents said they have received between 1 to 5 times, and 2 said between 6 to 10 times and another 2 respondents reported they have received more than 11 times (see Table4).

Table4: Frequency of receiving SMS by respondent

How frequent you have received the SMS?	**N**	**Respondent**
1 – 5 times	16	R3, R4, R5, R6, R7, R8, R9, R11, R12, R13, R14, R15, R16, R18, R19, R20
6 – 10 times	2	R2, R10
More than 11 times	2	R1, R17

To confirm the existence of fraudSMS, the respondents were asked about their awareness of fraudSMS. From Table 5, 15 respondents said they are aware about the fraudSMS, while another 5 respondents stated they were not aware of the SMS containing fraud elements the first time theyhave received it.

Table5: Respondent awareness in fraud SMS

Did you aware the SMS you have received is a fraud SMS?	**N**	**Respondent**
Yes, aware	15	R1, R2, R3, R4, R5, R6, R7, R8, R12, R13, R14, R15, R18, R19, R20
No, not aware	5	R9, R10, R11, R16, R17

iii) Fraudulent SMS (fraudSMS)

The following main research question is what guided the researcher of thisstudy to obtain the required data from the respondents. *What is defined by fraud SMS and its enthusiasm, power of influences, and impacts*

from the university student's perspective? Thefollowing three research questions were posed to supplement the central theme of the study,which was to identify the motivation, reasons and the impact of fraudulent SMS:

1) To discover the factors which motivate an individual to respond to fraud SMS.
2) To identify the reasons why victims are susceptible to fraud SMS
3) To recognize the impacts received by individuals who are victims of fraud SMS

Definition of fraud SMS

The interview process conducted towards the respondents and Table 6 below yield the result about the respondents' view in defining fraud SMS. The respondents were asked the question: "What do you understand about fraud through Short Message Service (SMS) or the Scam SMS?"The purpose of this question is to analyze the respondents' opinion and their understanding about fraud SMS.

The recorded information from the interviews was processed and thethemes were created for any ideas drawn out by the respondents along with the key phrases. There are six themes extracted from the interview data comprises of several key phrases under each theme. From the table the theme of victim's exploitation comprise the key phrases point out by respondents which is to obtain profit (5), take advantage (2) and causing damage to the victim (1). Under the deceitful SMS, cheating represents the highest number of key phrases stated by 7respondents when defining fraud SMS. There are 2respondents stated that fraud SMS is fake. Other respondents define fraud SMS is untrusted, contain manipulation and illegal activities mentioned by 1 respondent for each key phrases. There is also a respondent (1) who pointed out that if there is SMS stated that winning a trivia and competition or a lucrative reward (7) provide by the sender, it is also consider as fraud SMS. They agree that this type of SMS is unrealistic and illogical since they have never participated in any competition as mentioned by the sender. There are 2 respondents who stated that fraud SMS often uses local common number and 1 respondent stated fraudsters use private number to perform the fraud. The fraud SMS also attacks targeted victim mentioned by 2 respondents while 4 respondents stated that fraud SMS able to influence people that their number are lucky phone number that win certain competitions. There are 4 respondents assert that fraud SMS will request personal information such as bank account number and identity card number.

Table 6: Respondent defines fraud SMS

Key phrase	N	Respondent
Victim's exploitation	8	R1, R7, R8, R10, R13, R14, R15, R16,
Deceitful SMS	12	R1, R3, R6, R7, R8, R10, R11, R12, R13, R15, R16, R18
Unrealistic and illogical SMS	8	R1, R2, R3, R4, R5, R9, R14, R15
Sender's number	3	R15, R18, R19
Targeted receiver number	6	R1, R2, R12, R17, R18, R19
Request personal information	4	R13, R14, R19, R20

Enthusiasm in responding fraud SMS

In order to understand the enthusiasm of people responding to this kind of SMS, the researchershave asked the respondent a question; "In your opinion, what are the factors that force or encourage people to response to SMS contains fraud element?" Table 7 summarized 3 main factors emerged were attitude and behavior, financial problem and reward offer. There were 12 respondents who said it depends on the attitude and behavior of the receiver. A few personality traits have been identified such as, easily to get influenced, eager to try something new, lazy to work, less analytical, greed, and dare to take risk. Next, 12 respondents reported the receiver might have financial problem. They do not have steady income, desperate for money, and have debt. Other 12 respondents said some peoplehave the problems in their attitudes and behavior when someone is willing to take risk, lack of analysis, driven by greed and make hasty decision. There were 9 respondents who believed it is because of the reward offer as stated in the SMS. Usually, the reward offered is in a big amount such as cash money RM 10,000 or RM 20,000. Some SMS also offers luxury gift such as gadget like smart phone or car.

Meanwhile, 4 respondents reported experience by family, friends and relatives won any competition through SMS also play role to encourage receiver to response. There were 3 respondents stated because of company reputation and credibility as it involved big Companies like Petronas, Power Root, 100 PLUS and Shell. There were also 3 respondents believed the receiver might be influenced by other people who urge them to reply the SMS. And the rest of the respondents believed it is because of personal problem (2 respondents) and communication style, (1 respondent) such as using nice and pleasant words.

Table7: Factors motivate individual to response fraud SMS

Key phrase	**N**	**Respondent**
Company reputation and credibility	3	R10, R12, R13,
Reward offer	9	R1, R3, R6, R10, R11, R12, R14, R17, R19
Attitude and behavior	12	R4, R5, R6, R7, R8, R10, R12, R14, R15, R18, R19, R20
Financial problem	12	R2, R3, R4, R5, R7, R8, R9, R10, R14, R18, R19, R20
Experience by family, friends and relatives	4	R3, R4, R8, R12
Influence by other people	3	R2, R3, R4
Lack of knowledge and awareness	4	R1, R2, R4, R18
Personal problem	2	R2, R3
Communication style	1	R1

Power of influences in responding fraud SMS

It is believe that, people become victims to fraud SMS as they were influenced by several factors which drive them to respond towards those SMS. Therefore, a question was designed which asked the respondents: "In your opinion, why a person can be easily influenced and what influence individual response to SMS that contains the elements of fraud?" By referring to Table 8, there are three key phrases embrace the highest number of respondents. This includes 12 respondents which also the majority, agree that financial pressure or personal problem is the factor influence someone to response the fraud SMS. It is followed by 10 respondents stated that the attitude of the receiver which is not thinkingcarefully, easily influenced, make a hasty decision, risk taker, naive, materialistic, thought that it is a fortunate and greedyleads them to response those SMS.

Next, 9 respondents mentioned that rewards offered also drive people to response the fraud SMS. Other than that, 5 respondents point out lack of knowledge regarding fraud SMS can become the factor to influence people to response to the fraud SMS. The company reputation is also among the factors that can influence an individual to response fraud SMS since the company with robust reputation is well known and trusted by many people. Meanwhile, 3 respondents stated the sender's phone number which uses local number look promising for the victims and make them response to fraud SMS. The result also show two key phrases point out by 2 respondents for each which is the influence and support by friends and family, and the structure of words and sentence used is sufficient enough for the individual to response those SMS. There are three other factors can influence individual response to fraud SMS mentioned by 1 respondent for each factor. These factors are frequency of receiving SMS, other people's experience and a lack of analysis.

Table8: Power of influence drives someone response to fraud SMS

Key phrase	**N**	**Respondent**
Company reputation	4	R2, R3, R5, R7
Financial pressure / personal problem	12	R1, R3, R4, R6, R9, R10 , R11, R13, R16, R17, R18, R19
Frequency of receiving SMS	1	R3
Influence and support by friends and	2	R2, R4

family		
Lack of knowledge	5	R8, R12, R13, R15, R20
Other people's experience	1	R9
Rewards offered	9	R1, R2, R3, R4, R6, R7, R8, R9, R14
Sender's phone number	3	R2, R6, R9
Words and sentence structure	2	R4, R8
Attitude of receiver	10	R1, R4, R5, R10,R14, R15, R16, R17, R18, R20
Lack of analysis	1	R1

Impacts of fraud SMS

The fraud SMS is one of the criminal activities thus it must have contributed to negative impacts towards the victims. In this case, the researchers attempt to gather respondent's overview about the possible impact received by the individuals who response to fraud SMS. Therefore, the respondents need to answer the question of "In your opinion, what are the effects or consequences to the individual when they respond to fraud SMS?" The results are tabulated in the Table9 below. It can be seen that, as mentioned by 12 respondents, fraud SMS can affect the emotional and psychological of an individual if they response and become the victims. Meanwhile 6 respondents stated it can affect the physical and mental health which can make the victims to fall sick, demoralized, mental illness or to be worse if they attempt to commit suicide. In addition, 4 respondents claimed that the safety and privacy of an individual could also be affected if it involves the intimidation and threats by the fraud perpetrators towards the victims. Other impacts such as moral and ethic value, thinking and maturity level and affecting the study were reported by 3 respondents of each. Fraud SMS also can cause difficulties to the individuals where in this research, 8 respondents stated that among the personal difficulties involves financial and time wasting.

Table 9: Potential negative impacts to the victims of fraud SMS

Key phrase	**N**	**Respondent**
Emotional and psychological effects	12	R1, R2, R3, R4, R7, R8, R9, R11, R15, R16, R18, R19
Moral and ethic values	3	R9, R17, R18
Physical and mental	6	R1, R4, R6, R7, R8, R16
Family relationship	2	R2, R3
Safety and privacy	4	R7, R13, R17, R19
Affecting the study	3	R2, R3, R4
Thinking and maturity level	3	R9, R14, R20
Personal difficulties	8	R3, R4, R5, R7, R8, R10, R13, R19

iv) Fraud SMS avoidance and prevention method from respondent's perspectives

This research also attempts to gather respondent's view and opinion on how to avoid and prevent fraud SMS. The respondents were asked to provide their opinion on what is the possible method or technique thatcan be used in order to reduce the fraud occurrence or the victims. The question used in the interview was designed by the researchers mainly to answer the following research question:

1) To identify and determine the appropriate measures to avoid and prevent the problem of fraud SMS.

Avoidance

In order to obtain the required data, the researchers asked respondents "In your opinion, how individuals can avoid from getting involved or easily influenced by the fraud SMS?" This question has the purpose to

encourage respondents to generate their ideas by giving their opinion and judgement towards the issue. Table10 below shows the result of the respondents' judgement for this question. Majority respondents (12) claimed that, an individual should ignore the SMS and not to response to it. On the other hand, 9 respondents suggested that, one should make in depth analysis which can be done by asking family members or experienced personwho has received the SMS before. Other than that, individuals should also ask the communication agency or regulatory body to investigate the information received in SMS. The respondents also recommended that an individual should first verify the company or telecommunication provider whether the information is true or it has been exploited by other parties. The results find 6 respondents stated finding and gather more information through television, radio or internet also can make someone to become cautious about fraud SMS.

The respondents also added, by asking anybody who have the knowledge regarding to this issue can help someone to understand the syndicate and their modus operandi thus a preparation action can be prepared at initial stage. There are also 6 respondents give their opinions regarding to the security settings and firewall. These can be done by enhancing the system, security software and application by the individual or telecommunication provider. Some respondents also implies by filtering the malicious SMS using features in some of mobile phone can block the fraud SMS. There are 3 respondents who suggested making a report to the telecommunication provider, police and enforcement body such as Malaysian Communications And Multimedia Commission (MCMC) can avoid fraud SMS from becoming widespread. Meanwhile 2 respondents stated an individual must be alert and aware and 2 other respondents stated one must be knowledgeable about fraud SMS activities. Additionally, other 2 respondent suggest someone needs to take precautions actions and be more careful by avoiding any untrusted SMS or call from unknown number and not simply put high trust upon receiving SMS offering reward or win a certain competition.

Table 10: Ways to avoid fraud SMS

Key phrase	**N**	**Respondent**
Make in depth analysis	9	R1, R4, R5, R7, R9, R10, R11, R18, R20
Be alert and aware	2	R1, R2
Find and gather information	6	R1, R4, R7, R15, R16, R20
Be more careful	2	R2, R11
Be knowledgeable	2	R2, R19
Ignore the SMS	12	R3, R4, R6, R8, R9, R10, R11, R14, R15, R17, R18, R19
Security settings and firewall	6	R3, R13, R16, R18, R19, R20
Make a report	3	R8, R10, R17

Prevention

The researchers are interested to gain respondent's overview and opinion on the ways that can prevent fraud SMS. Therefore, respondents need to answer the questions of "In your opinion, what steps should be taken by an individual and any other responsible parties to raise awareness about the dangers of fraudulent activities through SMS?" The results are tabulated in Table11 below and majority respondents (17) stated that the information about fraud SMS must be circulated to the public. This can be done through spreading information on the internet, social networks (Facebook, Twitter, etc), provide notice at the bank or the ATM machine, creates commercial and clarification from company which has become the victims by the fraud SMS syndicate. It is followed by 13 respondents stated fraud SMS can be prevented through increase awareness level by undertaking the active campaign, public talks and conferences. Other than that, 9 respondents reported the telecommunication company should reveal any private numbers while any company which their name has been exploited by the fraudster must conduct a press conference in order to clarify the actual situation and to clear their names. While 7 respondents asserted that improving security system such as the features to filters and block SMS are necessary to prevent fraud SMS from being spread widely.

From the table, research on fraud SMS and elimination of telecommunication's agent are the least reported by 1 respondent for each. There are 6 respondents who suggested that mass media and the actions

of government plays important role in spreading information regarding fraud SMS. The Malaysian Communication and Multimedia Commission (MCMC) is the responsible agency to protect users in the matters of information and communication flows. The individual attitudes and behaviour also portray the prevention initiative of an individual. As mentioned by 5 respondents, individuals should ignore, be very careful, open minded, not greedy and hasty in making decision and not to put high trust upon receiving those SMS.One should also perform in depth analysis by asking other people or search relevant information on the internet. Next, 3 respondents stated that, a report to the enforcement body such as police and MCMC is needed in order to prosecute the fraudster and legal action can be carried out. Other than that, strengthening law enforcement and enforcers are essential to prevent the plague of fraud SMS. As suggested by 3 respondents, the initiative can begins byprohibiting parents to register phone number for their child below 18 years, while the police and MCMC should develop the innovative plan specialized on fighting the fraud SMS.

Table 11: Ways to prevent fraud SMS

Key phrase	**N**	**Respondent**
Action by government	6	R1, R4, R7, R8, R9, R13
Increase awareness level	13	R1, R2, R4, R9, R10, R11, R13, R14, R16, R17, R18, R19, R20
Perform in depth analysis	5	R7, R9, R10, R16, R20
Circulate information to public	17	R1, R2, R4, R5, R8, R9, R10, R11, R12, R13, R14, R15, R16, R17, R18, R19, R20
Advice by experienced people	4	R2, R4, R8, R14
Role of media	6	R3, R4, R5, R6, R10, R18
Individual attitudes and behavior	5	R3, R7, R10, R13, R16
Conduct more research on fraud SMS	1	R6
Action by telecommunication company	9	R6, R7, R8, R10, R11, R14, R15, R17, R19
Improve security system	7	R7, R8, R10, R13, R16, R19, R20
Roles of parents, family, friends and relatives	2	R8, R16
Report to enforcement body	3	R9, R15, R17
Elimination of telecommunication's agent	1	R10
Strengthening law enforcement and enforcers	3	R12, R14, R18

Conclusion and Recommendations

In this study, the researchers managed to gather diverse responses towards fraud SMS from the student's perspectives. Nowadays, the SMS service become as the integral tools in aiding people to communicate to each others for its convenience, easiness and cheaper rates. It is also become the medium for the fraudster perform their illegal activity such as fraud SMS. The findings from this study provide an insight about student's responsesfor the enthusiasm, motivation to response and impacts caused by fraud SMS. All respondents have experienced in receiving fraud SMS, some of them even become the victim by response the fraud SMS and suffered losses. The findings suggest that, a proactive awareness campaign is necessary to educate people about the risks in fraud SMS. The regulatory body, telecommunication service provider and the enforcement agency needs to develop strategic initiative to fight fraud SMS in more effective and efficient way as possible. Among others, an SMS filtering can be implemented as the initial step to avoid the fraud SMS reaching users. This can be conducted either directly on thephone or within the operator's network (Mulliner et al., n.d.). The incident of fraud SMS and the number of victims will be reduced if they are aware and able to take precaution actions once they receive the fraudulent SMS.

References

Affin Bank Berhad. (2013). Notis Amaran: Penipuan Dalam Komunikasi Telefon. [online]. Retrieved from: http://www.affinbank.com.my/BM/penipuan/telefon.htm.

Bank Simpanan Nasional. (2013). Notice. [online]. Retrieved from: http://www.mybsn.com.my/content.xhtml?contentId=257.

Brown, S. (2005).*Telecommunication Fraud Management.* Waveroad Securit.

Buehler, W. (2004).*Blocking of SMS Spam and Fraud: White Paper.* Nexus Telecom.

Central Bank of Malaysia. (2011). Beware of Fraudulent Telephone Calls, E-mails or SMS Requesting Personal Banking Information. [online].Retrieved from: http://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement_all&ac=98

Chete, F.O, Oyemade, D., Abere, R., Chiemeke, S.C. and Ima-Omasogie, I. (2012). Citizens Adoption of SMS Based E-Government Services in Lagos State, Nigeria. *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3, No. 4., p. 654-660.

Cloudmark. (2012). *Mobile Security Solutions Guide.*

Creswell, J. W. (2003). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

El Tawashi, H. A. (2010). *Detecting Fraud in Cellular Telephone Networks: Jawwal case study.*

International Telecommunication Union (ITU). (2005). ITU Survey On Anti-Spam Legislation Worldwide.*WSIS Thematic Meeting on Cybersecurity.* Document: CYB/06.

Irwan Dahnil& Salleh Esa.(2008). *Penipuan SMS yang perlu anda tahu.*

Kranacher Mary-Jo, Riley Jr., T. Wells .(2011). *Forensic Accounting and Fraud Examination.* John Wiley & Sons Inc.

Maharani A. C., Rosanna N., Liesman T. (2012).*The Adoption of SMS Technology in Disseminating Health Information in Indonesia: A Case Study on SMS Info Obat Murah and Nokia Life Healthcare Service.*

McAfee. (2013).*Mobile Security: McAfee Consumer Trends Repor: Trends in risky apps, mobile misbehavior, and spyware.* Mobile Security: McAfee Consumer Trends Report.

Morse, J. M., Barrett, M., Mayan, M., Olson, K., and Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, 1(2), 1-19.

Mulliner C., Golde N., and Seifert Jean-Pierre (n.d.). SMS of Death: from analyzing to attacking mobile phones on a large scale, Security in TelecommunicationsTechnische Universit ¨at Berlin and Deutsche Telekom Laboratories.

Murynets I., Jover R. P. (2012).*Crime Scene Investigation: SMS Spam Data Analysis, AT&T Intellectual Property.*

Puukangas K. M., TeliaSonera.(2010). *Fraud in Short Messaging in Mobile Networks.*

Stan Lester .(1999).*An introduction to phenomenological research.* Stan Lester Developments.

Strauss, A.& Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.). Thousand Oaks, CA: Sage.

Subex Telecom Fraud Alerts. (2012). Retrieved from: http://www.subex.com/fraud-alerts.html.

Tuckett, A. (2005). Part II. Rigour in qualitative research: Complexities and solutions.*Nurse Researcher*, 13(1), 29-42.

MOHAMAD RIDHUAN MAT DANGI, NORULHUDA TAJUDDIN
Universiti Teknologi MARA (Pahang).
ridhuan@pahang.uitm.edu.my, alhudatajuddin583@pahang.uitm.edu.my