Journal of Economics and Behavioral Studies (ISSN: 2220-6140)
Vol. 9, No. 5, pp. 255-264, October 2017

Plastic Money and Electronic Banking Services Espousal vis-a-viz Financial Identity Theft Fraud Risk Awareness in a Developing Country

Shewangu Dzomira
University of South Africa, Pretoria, South Africa
Great Zimbabwe University, Zimbabwe
shewangu@yahoo.com

Abstract: Exploitation of plastic money coupled with electronic banking services has come as expediency to financial establishment customers in Zimbabwe. This paper sought to analyze plastic money and electronic banking services espousal vis-a-viz financial identity theft fraud risk awareness in Zimbabwe banking sector via banks' websites. The theoretical underpinning for this study is Routine Activity Theory. The study used qualitative content analysis research technique for examination of the text content data through the consistent taxonomy process of coding and classifying themes or patterns to submit a painstaking considerate of financial identity theft fraud awareness by the banking sector in Zimbabwe. A sample size of 14 banks (including commercial, merchant and building societies) was used and the banks were arbitrarily chosen on the basis of website accessibility and ease of use of the data. The study findings suggest that there is very little financial identity theft awareness in Zimbabwe by the banking sector through their websites to the general public whilst there is amplified adoption of plastic money and electronic banking adoption. This study proposes a need to amplify the information and inform plastic card and electronic banking customers of the types of financial identity theft fraud. Plastic card and electronic banking is an urgent area to focus on for banking institutions and should inexorably capitalize in it. Financial identity theft information should be easily retrievable and conveyed in a manner that makes reasonableness to the varied customers.

Keywords: *Plastic money; electronic banking, identity theft; fraud risk*

1. Introduction

Financial liberalization and technology insurgency have endorsed the expansion of new-fangled and extra proficient release and dispensation means as well as more novel products and services in banking sector. Exploitation of plastic money coupled with electronic banking services has come as expediency to financial establishment customers. Plastic money[1] and electronic banking services have become a workable preference for financial service providers and customers interface. Plastic cards and electronic banking innovations have productively become an indispensable part of the up-to-the-minute transaction system, providing a wide array of services to the customers, and have achieved much recognition at global level and have considerably grown over the years (Pudaruth, Juwaheer & Madoo, 2013). However, the archetypal crime of the information epoch is identity theft[2], which refers to the malicious use of personal identifying data (Kahn & Roberds, 2008) or can be defined as the deliberate transfer, possession, or usage of any name or number that spots another person, with the target of perpetrating or assist a crime (Kahn & Liñares-Zegarra, 2013; Elbirt, 2005; Irfana & Raghurama, 2013). It is a type of impersonation that facilitates someone to perpetrate fraud and normally results in financial damage to the individual and financial gain to the impersonator (Radin, 2007). More so, financial identity theft involves the withdrawal of money by identity thief using personal information of a victim from his or her bank account and generally the victim is unaware that their identity has been stolen (Perl, 2003). This form of criminology is made feasible by the aforementioned contemporary payment systems where merchants are willing to tender goods and services to aliens in exchange for a guarantee to pay, provided the undertake is supported by data that tie the buyer to a particular account or credit history (Anderson, Durbin, & Salinger, 2008).

In other developed and emerging countries such as America and South Africa financial identity theft is the top growing crime, happening when the criminal gains confidential information from an individual or business

[1]Plastic money refers to the make use of credit or debit cards as a substitute for cash for goods and services payments.
[2] Identity theft, also known as identity fraud, happens when an individual's personally identifying information is used without permission and/or knowledge by someone else (often a stranger) (Radin, 2007).

and utilizes it to get right of entry into private financial accounts (Brody, Mulig & Kimball, 2007; Farina, 2015; Sanchez, 2012; Kahn & Liñares-Zegarra, 2013). Owing to the incessant technological progression and the nearly omnipresent use of electronic gadgets and the internet, financial identity theft is a crime that can take place virtually anywhere (Farina, 2015). This dawn of the information age has fashioned fresh challenges to the capability of individuals to guard the solitude and security of their personal information (Saunders & Zucker, 1999). Identity theft has become one of the most money-spinning criminal events eased by the capacious information obtainable on the internet and the reported episodes of identity theft have increased at an unmatched tempo (Elbirt, 2005; Aïmeur, & Schonfeld, 2011; Perl, 2003). Most customers are ignorant of the amount of data they divulge over the internet services proposed by search engines, social networking sites, e-commerce web sites and free online tools (Aïmeur, & Schonfeld, 2011). The increase of online services in which customers are confirmed by a username and password, is ever more browbeaten by identity theft actions (Moskovitch, Feher, Messerman, Kirschnick, Mustafić, Camtepe, & Elovici, 2009). Financial Identity theft fraud is a problem heart-rending the whole society and often is an entryway crime, in which stolen or fraudulent identities are used to steal money, claim eligibility for services, hack into networks without permission (Nokhbeh, Manoharan, Yang, & Barber, 2017).

Another titanic cost of financial identity theft, to businesses is the loss of customer confidence and therefore creating awareness is one of the most imperative outfits in fighting identity theft (Brody, Mulig, & Kimball, 2007). In addition financial institutions and consumers have to work in partnership to thwart further incidences. With sophisticated technology and unrelenting educational outreach by businesses, financial institutions and educational organizations, there will be a decrease in the level of identity theft taking place (Brody, Mulig & Kimball, 2007). As financial institutions progressively more offer online or electronic banking services and plastic card transactions to their customers, they must face issues of consumer trust in electronic service. If financial institutions, in cooperation with their customers, make it safe to adopt plastic and electronic services consequently, building the best controls to prevent fraud and protect customers is of significant magnitude (Irfana & Raghurama, 2013). There is extensive conformity that financial identity theft fraud causes financial smash up to consumers, lending institutions, retail establishments, and the economy at large (Hoofnagle, 2007).

Developing countries societies frequently experience derisory level of literacy when using electronic banking systems and it is apparent that except the financial organizations take all the indispensable and realistic steps to educate its clients, they stand a risk of paying robust indemnities for the loss of money online through identity theft (Granova & Eloff, 2004). Unpredictably, there is petite first-rate public information presented about the extent of the crime and the genuine damages it causes. Zimbabwe has not been an exception to the adoption of these innovations and the adoption has been driven by the recent liquidity challenges. The principal financial regulator, Reserve Bank of Zimbabwe have strongly encouraged espousal of plastic money (credit cards, debit card, visa card etc) and electronic innovations (Electronic Funds Transfer Systems (EFTs), mobile banking, personal computer, banking and internet banking). The usage of plastic cards and electronic transactions in Zimbabwe by customers and merchants has just dramatically increased. Nevertheless, adoption of plastic money and electronic innovations in Zimbabwe has not been related to the awareness and education on financial identity fraud security. It is therefore imperative for the financial institutions in Zimbabwe to give financial identity theft fraud awareness information to the general populace through disclosure on the websites. Against this backdrop this paper seeks to analyze plastic money and electronic banking services espousal vis-a-viz financial identity theft fraud risk awareness in Zimbabwe banking sector via banks' websites. The following sections of the paper covers contribution of the study, theoretical framework, empirical and literature review, methodology, findings and discussions, conclusion and implications.

Contribution of the study: This study makes a valuable contribution given the fact that qualitative empirical studies and literature on plastic money and electronic banking services adoption in relation to financial identity theft fraud risk awareness in the context of Zimbabwe as a developing nation are relatively very rare. Consequently, it would serve as a roadmap for banking institutions, regulators, policy makers and financial consumers to design strategies to better promote financial identity theft fraud risk awareness in Zimbabwe.

Theoretical Framework: The theoretical underpinning for this study is Routine Activity Theory which was coined by Cohen and Felson (1979). Crime is considered to be the corollary of the incidence of a stimulated offender, the presence of a suitable target, and the absence of a capable guardian (Hutchings and Hayes, 2009). Cohen and Felson (1979) suggested that there is an increased probability of victimization when individuals are positioned in high risk locations, are attractive targets, lack of a capable guardian and are in the reach of a motivated offender. Routine activity theory is traditionally drawn upon to underscore the role of offender motivation, target suitability, and effective guardianship in explaining victimization patterns (Drawve, Thomas & Walker 2014). Even though the routine activity approach was formerly written to account for direct-contact offenses, it seems that the viewpoint also has utility in elucidating crimes at a distance (Reyns, 2013).

Routine activity theory has been used to explicate cybercrime at individual level, but not at national level (Kigerl, 2012). According to Hutchings and Hayes (2009)'s findings indicate that potential victims who take on high levels of routine activities relating to computer and internet banking use are more probable to be attacked by motivated offenders. More so, Reyns (2013)'s results suggest that individuals who use the internet for banking are fairly more likely to be victims of identity theft than others. Correspondingly, online shopping and downloading behaviours augmented victimization risk. Reyns, Henson & Fisher (2011) found that specifically, antecedents measuring online exposure to risk, online immediacy to motivated offenders, online guardianship, online target charisma, and online deviance were noteworthy predictors of cyber aggravation victimization. However, Leukfeldt (2014) concluded that personal background and financial characteristics play no role in phishing victimization and only "targeted browsing" led to amplified risk. As for ease of access, using trendy operating systems and web browsers does not guide to superior risk, while having the latest antivirus software as a technically proficient guardian has no effect. The results showed no one has an augmented likelihood of becoming a victim. Consequently, banks could play the role of capable guardianship. There is therefore a need to pick identity theft earlier as Albrecht; Albrecht & Tzafrir (2011) found that if identity theft is detected before time, consumers can guard themselves from the immense and tricky costs of identity theft. Paek & Nalla (2015) in Korea their results propose that education level, routine online activities and fright of identity theft victimization are positively associated with identity theft persecution. Concurring to the above it was found that certain routine activities openly influence the possibility of encountering identity theft (Reyns & Henson, 2015).

2. Literature Review

In this modern world of information technology, many fraudsters prey on their fatalities via the internet given the level of revelation of personal information in many of current information age transactions. Two of the most frequent traditions that thieves obtain personal information to aid them in identity theft are phishing[3] and pharming (Brody, Mulig, & Kimball, 2007). Phishing employs mass e-mail messages to charm recipients into divulging personal information. The emails assert to be from one's bank or other organizations but are in fact would have been sent by fraudsters (Brody, Mulig, & Kimball, 2007; Irfana & Raghurama, 2013). These e-mails classically contain a link that takes the recipient to a phony website indistinguishable to the original website and one is asked to verify or update personal information. The personal information is taken by the fraudster who would use the information to access online bank account (Irfana & Raghurama, 2013). It is also known as web spoofing which involves fraudulent email and web sites that swindle gullible users into disclosing confidential information (Chou, Ledesma, Teraguchi & Mitchell, 2004). Phishing is a form of social engineering based on technical exploits (for instance, password sniffers intercepting encrypted passwords and key loggers capturing the victim's keystrokes) or a blend of both technology and social engineering (Hutchings and Hayes, 2009).

[3] The word "phishing" comes from an analogy to fishing; the email is bait used to lure in "fish" from the "sea" of internet users. The "f" is changed to "ph" in keeping with computer hacking tradition (Lynch 2005:259)

Social engineering practices (Spear Phishing, Pharming and Smishing) are most habitually used where perpetrators fake as legitimate companies appealing for personal details targeting profiled groups based on needs for goods and services, getting better their success; bypass social engineering, as a substitute targeting software ensuing in the automatic redirection to illegitimate mock websites; and use SMS text messages to aim mobile internet users (Williams, 2015). In a similar scheme Vishing involves a person calls pretending to be a bank representative seeking to verify account information (Irfana & Raghurama, 2013). Pharmers, on the other hand, shed a broad net for the credulous (Brody, Mulig, & Kimball, 2007). Pharming is the installation of malicious code on one's computer without any acknowledgement or an e-mail attachment that installs malicious code on a computer which leads to a fake website insecurely resembling bank's website and without knowledge one provide financial identity details (Irfana & Raghurama, 2013). Moreover, electronic banking credentials can also be gained by malware that is fixed on computers without users' knowledge, normally by clicking on a link allied to fouled software in an unsolicited email (Williams, 2015). Malware has been intended to log users' keystrokes, insert fake web pages (browser in the middle attack) and execute illicit actions on computers, in an endeavour to capture passwords and personal banking information (Williams, 2015). Malware includes keyloggers and spyware. Spyware is installed on a victim's computer and with the use of a keylogger permits a fraudster to not only spy on what websites are visited, but also record what keys are hard-pressed such as online banking passwords (NSW Justice, 2011).

On the other hand, plastic card fraud is defined as using plastic payment cards, such as ATM, debit, credit or store cards to withdraw money without permission or prior knowledge from a financial institution (NSW Justice, 2011). Plastic card fraud frequently happens via the illegitimate gaining and/or use of card information and the personal identification number (NSW Justice, 2011). In most cases cards used to commit fraud are usually lost or stolen cards which could be used intact or changed by re-embossing and re-encoding, or forged cards that are completely new (Smith & Grabosky, 1998). To counterfeit a card it is essential to know the details of an existing legitimate cardholder consequently the craving of reprobate to acquire rightful plastic card details from other sources such as the internet (Smith & Grabosky, 1998). Occasionally information on the card's magnetic strip is obtained through "card skimming". This is when a genuine card is obtained for a few seconds to facilitate it to be passed over a magnetic tape reader so that a phoney copy may be made (Smith & Grabosky, 1998). Another technique is "buffering", which entails transforming the information kept in the magnetic strip of the card or gaining security codes electronically (Smith & Grabosky, 1998). Nonetheless, according to Pudaruth, Juwaheer & Madoo (2013) in their analysis they revealed that customers have acknowledged plastic cards as a helpful means of effecting payments since plastic cards proffers worldwide acceptance. Even though plastic cards are valuable, Sakharova & Khan (2011) found that payment card fraud is causing billions of dollars in losses for the card payment industry and the brand name can be affected by loss of consumer buoyancy due to the fraud. This requires the supply of awareness information as Vincent (2005) concluded that provision of information about credit card functioning in India and payment settlement is a good thing to both the merchants and customers. In the same vein Kaseke (2012) found that individual factors such as education level had a bearing on the use of plastic money. In support to that Archer (2012) implicated that consumer education on identity theft fraud leads to pressure that consumers need to utilize all behaviours that can reduce risk and loss.

Irfana & Raghurama (2013) concluded that many individuals or organizations are not observant enough and do not take proper safety measures whilst online. Subsequently, this directs to fraudsters detaining their personal information and performing all types of fraudulent transactions on the internet. For this reason, users of e-banking should make sure that they follow protected principles when giving away or accessing sensitive information. Moir & Weir, (2009) specifically found that a predominantly high occurrence of agents who had before dealt with phone calls that they measured doubtful. Moreover, there were agents within such surroundings who had previously been presented money in exchange for customers' details, or who know of beneficiary workers who received such offers. Ultimately, they found that specific practices within contact centres may add to the probability of identity theft. All in all, Milne (2003) concluded that identity theft is a severe and progressively more ubiquitous crime, and consumers need to take precautionary measures to lessen the chance of becoming a victim and that consumer education appears to be satisfactory for several identify theft preventative behaviours. Steyn, Kruger & Drevin (2007) found that educational and awareness activities pertaining to email environments are of utmost significance to manage the amplified risks of identity theft. Dzomira (2016) found that internet fraud awareness to the general public via website is

stumpy by many Southern African banks. Even though some banks have internet fraud information on internet banking applications, however, the bona fide usefulness of this information is timid.

3. Methodology

The study used qualitative content analysis research technique for examination of the text content data through the consistent taxonomy process of coding and classifying themes or patterns Du-Plooy-Cilliers, Davis, & Bezuidenhout (2014) to submit a painstaking considerate of financial identity theft fraud awareness by the banking sector in Zimbabwe in the wake of espousal of plastic money and electronic services. A sample size of 14 banks (including commercial, merchant and building societies) was used and the banks were arbitrarily chosen on the basis of website accessibility and ease of use of the data. The sample size was premeditated considering the exactitude of how closely the sample value relates to the population value of 19 banks (commercial, building societies, merchant and savings bank) and suggested 'equal precision' of 10% (Brink et al., 2013) and, in this study, 74% (14 banks) of the total population was used as the sample size. Information on plastic money and electronic services banking fraud awareness was retrieved from each bank's website in the sample size. QDA Miner a qualitative data and text analysis software package was used for coding textual data and annotating, retrieving and reviewing coded data and documents. Coding sequence was done on the salvaged libretto marking sections of data. The descriptive statistical analysis was done using frequencies, cluster analysis, similarity matrices, and crosstab matrix.

4. Findings and Discussion

Adoption of Plastic Cards and Electronic Banking: The table below shows the espousal of plastic cards and electronic banking by the 11 banks constituting the sample size. The scoring of the variables was basically dichotomous, where a variable scores 1 if adopted and 0 if it is not. The results suggest that all the 11 banks (100%) have adopted the use of plastic cards and electronic banking services in Zimbabwe.

Table 1: Adoption of Plastic Cards and Electronic Banking

Bank	Plastic Card Adoption		Electronic Banking Adoption	
	Score	%	Score	%
Bank 2	1.00	100%	1.00	100%
Bank 3	1.00	100%	1.00	100%
Bank 4	1.00	100%	1.00	100%
Bank 5	1.00	100%	1.00	100%
Bank 6	1.00	100%	1.00	100%
Bank 7	1.00	100%	1.00	100%
Bank 8	1.00	100%	1.00	100%
Bank 10	1.00	100%	1.00	100%
Bank 11	1.00	100%	1.00	100%
Bank 13	1.00	100%	1.00	100%
Bank 14	1.00	100%	1.00	100%
Total	11	100%	11	100%

Financial Identity Theft Fraud Risk Awareness Coding frequencies: Coding frequencies from Table 1 below constitute the list of all codes in the codebook along with their category to which they belong. It was found that phishing/pharming has the highest count of 7 (26.90%) in 7 (50%) cases. This shows that only seven banks out of 14 banks have disclosed phishing/pharming awareness on their websites to the general public. Malware and vishing have 3 counts (11.5%) each and from 3 cases (21.4%) each followed by hacking/cracking, key-logging, and lost/stolen card with 2 counts (7.7%) each from 2 cases (14.3%) each and lastly skimming, smshing, social engineering, swim swap fraud, card cloning, 419 scam and ATM card fraud with 1 count (3.8%) each from 1 case (7.1%) each. These results suggest that the bulk of the banks in the sample size have no disclosure of all the identified financial identity theft fraud types hence all the banks in the sample size have adopted plastic card and electronic banking services. This also suggests that the banks need to increase the awareness of financial identity theft risk as this would adversely affect the full implementation of plastic money and electronic banking services. The results concur with Kahn & Liares-

Zegarra (2016)'s findings that certain forms of identity theft episodes affect positively the probability of espousing credit cards, stored value cards, bank account number payments and online banking bill payments. More so, Geeta (2011)'s findings suggest that there has been an augment in identity theft in the last few years which could pose a grave quandary in the future, resulting in loss of confidence by the customer towards internet banking.

Coding co-occurrence similarity: The co-occurrence similarity index shown in Table 2 below allows the selection of the similarity measure used in clustering. Ochiai's coefficient measures the mere occurrences of specific codes in a case without considering their frequency. Ochiai's coefficient index is the binary form of the cosine measure which is represented by *SQRT (a^2/((a+b)(a+c)))*, where *a* represents cases where both items occur, and *b* and *c* represent cases, where one item is present but not the other one. From Table 2 below 419 scam and ATM fraud; ATM card fraud and card cloning; 419 scam and skimming; ATM card fraud and skimming; and card cloning and skimming have a coefficient of 1 each indicating that they occur more often. Vishing and key-logging have the second highest coefficient of 0.816 followed by swim swap fraud and hacking/cracking with a coefficient of 0.707. From the results there is an indication that the bulk of the combinations have a nil coefficient reflecting that the disclosure is very low.

Table 2: Coding frequencies

Category	Code	Count	% Codes	Cases	% Cases
Financial Identity Theft Fraud	Phishing/Pharming	7	26.90%	7	50.00%
Financial Identity Theft Fraud	Malware	3	11.50%	3	21.40%
Financial Identity Theft Fraud	Skimming	1	3.80%	1	7.10%
Financial Identity Theft Fraud	Smshing	1	3.80%	1	7.10%
Financial Identity Theft Fraud	Vishing	3	11.50%	3	21.40%
Financial Identity Theft Fraud	Hacking/Cracking	2	7.70%	2	14.30%
Financial Identity Theft Fraud	Key logging	2	7.70%	2	14.30%
Financial Identity Theft Fraud	Social Engineering	1	3.80%	1	7.10%
Financial Identity Theft Fraud	Lost/Stolen Card	2	7.70%	2	14.30%
Financial Identity Theft Fraud	SIM swap fraud	1	3.80%	1	7.10%
Financial Identity Theft Fraud	Card cloning	1	3.80%	1	7.10%
Financial Identity Theft Fraud	419 Scam	1	3.80%	1	7.10%
Financial Identity Theft Fraud	ATM card fraud	1	3.80%	1	7.10%

Table 3: Coding co-occurrence similarity

	419 Scam	ATM card fraud	Card cloning	Hacking/Cracking	Key-logging	Lost/Stolen Card	Malware	Phishing/Pharming	SIM swap fraud	Skimming	Smshing	Social Engineering	Vishing
419 Scam	1												
ATM card Fraud	1	1											
Card cloning	1	1	1										
Hacking/ Cracking	0	0	0	1									
Key-logging	0	0	0	0.5	1								
Lost/ Stolen Card	0	0	0	0	0	1							
Malware	0	0	0	0.408	0.408	0	1						
Phishing/ Pharming	0	0	0	0.535	0.535	0	0.436	1					

SIM swap fraud	0	0	0	0.707	0	0	0.577	0.378	1				
Skimming	1	1	1	0	0	0	0	0	0	1			
Smshing	0	0	0	0	0	0	0	0.378	0	0	1		
Social Engineering	0	0	0	0	0	0	0	0.378	0	0	0	1	
Vishing	0	0	0	0.408	0.816	0	0.333	0.655	0	0	0.577	0	1

Case similarity matrix: Table 3 above shows clustering performed on banks; the matrix used for clustering consists of cosine coefficients computed on the relative frequency of the various financial identity theft fraud types' awareness. The more corresponding two cases will be in terms of the share of codes the higher will be the coefficient. Comparisons were based on which codes appear in each case, without taking into account the number of times each code appears. From the results Bank 7 and Bank 10; and Bank 8 and Bank 11 clusters have highest coefficient of 1 each. This means that the corresponding banks have similar financial identity theft fraud disclosures. Bank 6 and Bank 8; and Bank 6 and Bank 11 clusters follow with a coefficient of 0.84 each and the least coefficient is 0.28 belonging to Bank 13 and Bank 14 cluster; Bank 4 and Bank 14 cluster, and Bank 3 and Bank 14 cluster.

Table 4: Case similarity matrix

	Bank 2	**Bank 3**	**Bank 4**	**Bank 5**	**Bank 6**	**Bank 7**	**Bank 8**	**Bank 10**	**Bank 11**	**Bank 13**	**Bank 14**
Bank 2	1										
Bank 3	0.72	1									
Bank 4	0.4	0.82	1								
Bank 5	0.42	0.71	0.71	1							
Bank 6	0.44	0.59	0.59	0.64	1						
Bank 7	0.46	0.4	0.4	0.42	0.44	1					
Bank 8	0.46	0.72	0.72	0.76	0.84	0.46	1				
Bank 10	0.46	0.4	0.4	0.42	0.44	1	0.46	1			
Bank 11	0.46	0.72	0.72	0.76	0.84	0.46	1	0.46	1		
Bank 13	0.72	0.64	0.64	0.52	0.59	0.4	0.72	0.4	0.72	1	
Bank 14	0.4	0.28	0.28	0.32	0.36	0.4	0.4	0.4	0.4	0.28	1

Cross tabulation matrix: The dialog box, Table 4 above explores the correlation between financial identity theft fraud awareness and banks in Zimbabwe as defined by values of categorical variable. The dialog box counts the total number of times financial identity theft fraud awareness has been unveiled by each bank making the sample size. The top most exhibits are shown by Banks 14; 13; 4 and 3 with 4 counts each of the financial identity theft fraud types out of 12 types. Bank 5 has 3 counts only whilst Bank 6 has 2 counts and the rest have 1 count each. The results propose that there is very low disclosure of financial identity theft fraud by banks in Zimbabwe whilst all the banks comprising the sample size have adopted plastic money and electronic banking services for their customers. The banks are not adequately providing financial identity theft awareness to the general public on their websites.

Table 5: Cross tabulation matrix

	Bank 2	**Bank 3**	**Bank 4**	**Bank 5**	**Bank 6**	**Bank 7**	**Bank 8**	**Bank 10**	**Bank 11**	**Bank 13**	**Bank 14**	**Pear-son's R**	**P value**
Phishing/ Pharming	0	1	1	1	1	0	1	0	1	1	0	-0.138	0.342
Malware	1	1	0	0	0	0	0	0	0	1	0	-0.246	0.233
Skimming	0	0	0	0	0	0	0	0	0	0	1	0.531	0.047
Smishing	0	0	0	1	0	0	0	0	0	0	0	-0.209	0.268
Vishing	0	1	1	1	0	0	0	0	0	0	0	-0.564	0.035

Hacking/ Cracking	0	0	1	0	0	0	0	0	0	1	0	0.117	0.366
Key-logging	0	1	1	0	0	0	0	0	0	0	0	-0.496	0.06
Social Engineering	0	0	0	0	1	0	0	0	0	0	0	-0.127	0.355
Lost/ Stolen Card	0	0	0	0	0	1	0	1	0	0	0	0.117	0.366
SIM swap fraud	0	0	0	0	0	0	0	0	0	1	0	0.448	0.083
Card cloning	0	0	0	0	0	0	0	0	0	0	1	0.531	0.047
419 Scam	0	0	0	0	0	0	0	0	0	0	1	0.531	0.047
ATM card fraud	0	0	0	0	0	0	0	0	0	0	1	0.531	0.047
Total	1	4	4	3	2	1	1	1	1	4	4		

Generally, the study's results are supported by other scholars' findings and conclusions. Vincent (2005)'s study conclusion that provision of information about credit card functioning in India and payment settlement is a good thing to both the merchants and customers. Also the results correspond with Kaseke (2012)'s findings that individual factors such as education level had a bearing on the use of plastic money and that a number of problems were encountered by consumers in relative to security. Archer (2012)'s findings correspond with this study's results. The results implicated that consumer education and awareness on identity theft and fraud leads to pressure that consumers need to utilize all behaviours that can reduce risk and loss. Moreover, the findings support Milne (2003)'s conclusion that consumer education appears to be satisfactory for several identify theft preventative behaviours. The findings concur with Steyn, Kruger & Drevin (2007) who found that educational and awareness activities pertaining to email environments are of utmost significance to manage the amplified risks of identity theft. As well, Dzomira (2016) found that internet fraud awareness to the general public via website is stumpy by many Southern African banks. Even though some banks have internet fraud information on internet banking applications, however, the bona fide usefulness of this information is timid.

5. Conclusion

It is therefore concluded that there is very little financial identity theft awareness in Zimbabwe by the banking sector through their websites to the general public against an amplified adoption of plastic money and electronic banking services. This study proposes a need to amplify financial identity theft awareness information and enlighten plastic card and electronic banking customers of the types of financial identity theft fraud they are likely to encounter. Plastic card and electronic banking is an urgent area to focus on for banking institutions and should inexorably capitalize in it. Financial identity theft information should be easily retrievable and conveyed in a manner that makes reasonableness to the varied customers. Also, to curb financial identity theft risk linked with plastic card and electronic banking activities conducted both locally and externally, banks should make ample disclosure and consciousness of financial identity theft information on their web sites to the universal public and take apt measures to warranty adherence to financial customer privacy requirements relevant in the jurisdictions to which the bank is providing plastic card and electronic banking services. More so, it is concluded that Routine activity theory is incomparable among theories of criminology in that it seek out to expound changing plastic card and electronic banking fraud hounding risks among individuals and the accountability of illicit location in the episode of criminal events committed online. At the heart of routine activity theory is the thought that crimes can only grow when three fundamentals of a situation are in existence: plastic card and electronic fraudsters, plastic card and electronic users, and ineffectual financial guardians. When these three situational bare bones come together in place and time, the likelihood of plastic card and electronic banking fraud event happening is significantly amplified predominantly in the deficiency of awareness.

Study Implications: This study affords a profound understanding on financial identity theft awareness factor impacting on plastic card and electronic services embracing. This study proposes a policy by banking regulators or overseers in Zimbabwe for increasing the financial identity theft fraud awareness information and informs financial customers of plastic card and electronic fraud committed by fraudsters. The information must be out in the open to the general public on the website of each banking institution not only to offer such information, when a customer has logged in on the internet application to transact. This would make plastic card and electronic banking fraud material readily retrievable. Moreover, banking regulators in Zimbabwe must pass regulations that make banking institutions to take apt measures to ensure adherence to customer privacy requirements applicable in the country. The banking regulators also should make policies towards the prioritization of financial identity theft fraud risk by banks on their risk registers. That is the banking institutions, therefore, should prioritize financial identity theft fraud risk aspects on banking institution's risk register so as to stand competitive advantage in the contemporary technologically sophisticated epoch.

References

Anderson, K. B., Durbin, E. & Salinger, M. A. (2008). Identity Theft. *Journal of Economic Perspectives*, 22, 171–192. doi:10.1257/jep.22.2.171

Albrecht, C., Albrecht, C. & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime*, 18, 405–414. doi:http://dx.doi.org/10.1108/13590791111173722

Aïmeur, E. & Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. In 2011 9th Annual International Conference on Privacy, Security and Trust, PST 2011 (pp. 24–31). doi:10.1109/PST.2011.5971959

Archer, N. (2012). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*. doi:10.1108/13590791211190704

Brody, R. G., Mulig, E. & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, 11, 43–56.

Chou, N., Ledesma, R., Teraguchi, Y. & Mitchell, J. C. (2004). Client-side defense against web-based identity theft. NDSS, 1–16. doi:10.1.1.65.679

Du-Plooy-Cilliers, F., Davis, C. & Bezuidenhout, R. (2014). *Research Matters*. Juta & Company, South Africa.

Drawve, G., Thomas, S. A., & Walker, J. T. (2014). The Likelihood of Arrest: A Routine Activity Theory Approach. *American Journal of Criminal Justice*, 39, 450–470. doi:10.1007/s12103-013-9226-2

Dzomira, S. (2016). Financial consumer protection: internet banking fraud awareness by the banking sector. *Banks and Bank Systems*, 11(4).

Elbirt, A. J. (2005). Who Are You? How to Protect Against Identity Theft. IEEE Technology and Society Magazine, 24, 5–8. doi:10.1109/MTAS.2005.1442375

Farina, K. A. (2015). Cyber Crime: Identity Theft. *International Encyclopaedia of the Social & Behavioral Sciences (Second Edition)*, 5, 633–637. doi:http://dx.doi.org/10.1016/B978-0-08-097086-8.45054-3

Geeta, D. V. (2011). Online identity theft – an Indian perspective. *Journal of Financial Crime*, 18, 235–246. doi:10.1108/13590791111147451

Granova, A. & Eloff, J. (2004). Online banking and identity theft: Who carries the risk? Computer Fraud and Security. doi:10.1016/S1361-3723(04)00134-4

Hutchings, A. & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation. *Current Issues in Criminal Justice*, 20(3).

Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law & Technology*, 21, 98–122.

Irfana, S. & Raghurama, A. (2013). Innovation in Indian Banking: Extent of Precautions Taken By the Customers While E-Banking. *IOSR Journal of Business and Management (IOSR-JBM)*, 8(5), 01-09

Kahn, C. M. & Liñares-Zegarra, J. M. (2013). Identity Theft and Consumer Payment Choice: Does Security Really Matter?

Kahn, C. M. & Roberds, W. (2008). Credit and identity theft. *Journal of Monetary Economics*, 55, 251–264. doi:10.1016/j.jmoneco.2007.08.001

Kahn, C. M. & Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter? *Journal of Financial Services Research*, 50, 121–159. doi:10.1007/s10693-015-0218-x

Kaseke, N. (2012). Cash or Plastic Money – An Investigation into the Payment Mode Post Multi-Currency Period in Zimbabwe. *International Journal of Advanced Research in Management and Social Sciences*, 1(6).

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30, 470–486. doi:10.1177/0894439311422689

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. *Cyberpsychology, behavior and social networking*, 17, 551–5. doi:10.1089/cyber.2014.0008

Milne, G. R. (2003). How well do consumers protect themselves from identity theft? Journal of Consumer Affairs. doi:10.1111/j.1745-6606.2003.tb00459.x

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafić, T., Camtepe, A. & Elovici, Y. (2009). Identity theft, computers and behavioral biometrics. In 2009 IEEE International Conference on Intelligence and Security Informatics, ISI 2009 (pp. 155–160). doi:10.1109/ISI.2009.5137288

Moir, I. & Weir, G. R. S. (2009). Contact centres and identity theft. *International Journal of Electronic Security and Digital Forensics*, 2(92). doi:10.1504/IJESDF.2009.023879

Nokhbeh-Zaeem, R., Manoharan, M., Yang, Y. & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers and Security*, 65, 50–63. doi:10.1016/j.cose.2016.11.002

NSW. (2011). Background paper: plastic card fraud

Paek, S. Y. & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, 43, 626–642. doi:10.1016/j.ijlcj.2015.02.003

Perl, M. W. (2003). It's not always about the money: When the state identity theft laws fail to adequately address criminal record identity theft.

Pudaruth, S., Juwaheer, T. D. & Madoo, V. (2013). Mapping the Hidden Constructs towards the Adoption of Plastic Cards in Mauritius. *International Journal of Advanced Research*, 1(4), 340-355

Radin, T. J. (2007). Identity Theft. In Encyclopaedia of Business Ethics and Society (p. 2592).

Reyns, B. W. & Henson, B. (2015). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology*, 1, 1–21. doi:10.1177/0306624X15572861

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50, 216–238. doi:10.1177/0022427811425539

Reyns, B. W., Henson, B. & Fisher, B. S. (2011). Being Pursued Online: Applying Cyber lifestyle-Routine Activities Theory to Cyber stalking Victimization. *Criminal Justice and Behavior*, 38, 1149–1169. doi:http://dx.doi.org.ezproxy.uky.edu/10.1177/0093854811421448

Sakharova, I. & Khan, L. (2011). Payment Card Fraud: Challenges and Solutions, Technical Report - UTDCS3411, The University of Texas at Dallas, Department of Computer Science, Selected Papers in Security Studies: Volume 5, The University of Texas at Dallas, PP No. 1 - 25.

Sanchez, M. (2012). the Role of the Forensic Accountant in a Medicare Fraud Identity Theft Case. *Global Journal of Business Research (GJBR)*, 6, 85–92.

Saunders, K. M. & Zucker, B. (1999). Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *Cornell Journal of Law and Public Policy*, 13, 183–192. doi:10.1080/13600869955134

Smith, R. G. & Grabosky, P. (1998). Plastic Card Fraud. Australian Institute of Criminology. Paper presented at the conference Crime Against Business, convened by the Australian Institute of Criminology, held in Melbourne 18 – 19 June 1998

Steyn, T., Kruger, H. A. & Drevin, L. (2007). Identity theft - Empirical evidence from a phishing exercise. *In IFIP International Federation for Information Processing*, 232, 193–203). doi:10.1007/978-0-387-72367-9_17

Vincent, L. (2005). Credit Cards - Modem Payment System. *Review of Social Sciences*, VI(1), 71-76.

Williams, M. L. (2015). Guardians upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. Brit. J. Criminol. 56, 21–48