Exploring the challenges of forensic technology in responding to credit card fraud in Sedibeng Region, South Africa

Motseki Morero Moses(a)* Mofokeng Jacob Tseko(b)

(a)Postdoctoral Fellow, Faculty of Humanities, Department of Safety and Security Management, Tshwane University of Technology, 2 Aubrey Matlakala St, Soshanguve, Pretoria, 0001, South Africa.
(b)Professor, African Research Chair for the Campus and School Public Safety, Faculty of Humanities, Department of Safety and Security Management, Tshwane University of Technology, 2 Aubrey Matlakala St, Soshanguve, Pretoria, 0001, South Africa.

Abstract

Today use of Credit Card even in developing countries has become a common scenario. People use it to shop, pay bills and for online transactions. This study explored the challenges of forensic technology in responding to credit card fraud as an approach used by the South African Police Service (SAPS) in Sedibeng region. This study was carried out utilizing a qualitative approach and thirty nine interviews were carried out among officials deployed in the SAPS, community leaders, members of the community and bank managers. The key findings indicated that the challenges in responding to this scourge is that the perpetrators utilise advanced technologies resources (computer hacking software) as opposed to SAPS which does not have systems nor capacity to effectively respond to this crime. The limited resources to respond to this crime adequately. For recommendations; significant emphases should be directed on the promotion of public awareness through public education. The intensive training of SAPS officials and inter-governmental collaboration between the SAPS, community police forums, bank managers and South African Banking Risk Information Centre (SABRIC) in understanding this technology are highly advised.

Keywords: Credit card fraud, Forensic technology, Policing, Sedibeng region, South Africa.

JEL Classification: O35

Introduction

Card payments in South Africa continue to be a predominant part of the National Payments System in an evolving payments ecosystem. Due to the growing volume of electronic payments, the monetary strain of credit card fraud is turning into a substantial challenge for financial institutions and service providers, thus forcing them to continuously improve their fraud detection systems (Maluleke, Motseki, Mokwena & Dlamini, 2021). According to (Ishu & Mrigya, 2016), credit card is a thin handy plastic card that contains identification information such as a signature or picture, and authorises the person named on it to charge purchases for which he/she will be billed periodically. Motseki (2021) concurs that today utilisation of Credit Card even in non-industrial nations has become a typical situation. Individuals use it to shop, cover tabs and for online exchanges.

The introductory part of this study revealed that a credit card is a convenient method of payment, but it does carry risks. The enormous growth in the use of credit cards has resulted in high levels of credit card fraud. Based on the abovementioned background, the use of credit cards has become a way of life in many parts of the world. There is a rapid growth in the number of credit card transactions which has led to a substantial rise in fraudulent activities (Ishu & Mrigya, 2016). South African Banking Risk Information Centre (2017) concurs that today, credit cards are used like cash. All credit cards have one thing in common, namely that the bearer can obtain something of value simply by presenting the card. However, credit card fraud results in high losses both for the banking industry and consumers and seems to be increasing (Maluleke et al, 2021). The purpose of this article was to explore the challenges
of forensic technology in responding to credit card fraud as an approach used by the South African Police Service (SAPS) in Sedibeng region and to evaluate the availability of technological and conventional resources to respond to this scourge, as well as the capabilities of the SAPS to utilise the available [lack of forensic technology] resources to respond best to credit card fraud.

This paper aims at exploring the challenges of forensic technology in responding to credit card fraud as an approach used by the South African Police Service (SAPS) in Sedibeng region. This study was carried out utilising a qualitative approach and thirty nine interviews were carried out among officials deployed in the SAPS, community leaders, members of the community and bank managers.

**Conceptual Background**

**Credit Card Fraud: Forensic Technology Measures**

There is a virtual arms race taking place online between financial institutions and cyber criminals, who as soon as the bank deploys a new process or technology to prevent online fraud, they find a weakness to exploit (ACI, 2013; Dzomira, 2014). In addition, customers expect to be protected from fraud, but also want anti-fraud tools to look at them holistically, assessing the credit card fraud risk of transactions based on their individual profiles. Five ways to combat credit card frauds are highlighted below as:

**Adopt appropriate technologies**

According to Bhasin (2016) an inclusive mix of strong authentication systems; analytics software; and bank services, positive pay and payee verification, for example, can greatly reduce an organization’s exposure to fraud. It is important to have layers of protection. The researchers are of the view that it is very important for the police to also hire IT specialists and experts in computer sciences to ensure that the necessary skills and knowledge are available and in available in the police ranks. The banks, SABRIC and the police need to form a multi-disciplinary team that would work together throughout South Africa to fight this scourge (Bhasin, 2012).

**Beef up your internal controls:** Sarbanes-Oxley mandates that companies pay strict attention to their internal controls. But even the most thorough Sarbanes-Oxley compliance effort cannot provide comprehensive protection against credit card fraud. Proactive organizations will want to put additional controls in place, including rigorous approval procedures and careful separation of duties (Bhasin, 2016). That is especially true of disbursement processes, such as wire transfers. The researchers are of the view that most of the credit card incidents or crimes are linked with the individuals who works from the internal part of the banks, they release confidential information about the clients to the perpetrators of this crime. Internal controls need to be prioritised and external auditors or investigators need to check and monitor those working internally (Maluleke et al, 2021).

**Screen job applicants carefully:** according to Premium (2018) one of the biggest security problems company’s face is fraud perpetrated by trusted insiders. Key finance functions such as treasury must conduct background checks on potential hires, and companies should also consider drug testing and honesty testing. It is the first line of defense.

**Educate your workforce:** Employees need to understand how damaging fraud can be to the organization. They must be able to recognize signs of fraudulent activity and know how to report it. In addition, treasury employees will need to be trained in the correct use of the company's fraud-protection tools and technologies (SABRIC, 2017).

**Prosecute thieves:** Many organizations fire employees who are caught stealing but avoid prosecuting them for fear of bad publicity. A zero-tolerance policy goes a long way toward reducing the risk of illegal activity. Likewise, managers should immediately turn over any evidence of suspected fraud to law enforcement agencies (Bhasin, 2016).

**Forensic technology models to improve the law enforcement response to credit card fraud**

**Education through Community Outreach**

Many victims may not know what to do once they discover that they have been victimised, or that swift action on their part may minimise the damage done. Local police, as part of their outreach programmes, may help in educating consumers concerning these matters and steps they can take both to avoid their victimisation and to report their victimisation should it occur. Many police departments now have information on their web sites and some offer online ways of reporting victimisation. Directing victims to internet resources or providing them written materials that explain how the recovery process works may help in reducing victim's suffering, Albrecht, Albrecht, and Tzafrir (2011).

In support of this statement, when considering the current state of police partnership with the public in South Africa, the researchers are of the perception that it will take more than community will outreach programmes by police to indeed educate the public about ID theft. This is simply based on the researchers’ observations that the partnership between the public and the SAPS has gradually been dented, and to convey information regarding ID theft, police will first have to ensure that the public trust in their services is gained. The public needs to understand that police existence in their community is to uphold the law and maintain security, and this can only be done if the number of police corrupt cases maybe, if possible combated (SABRIC, 2019).
Effective Communication

The most common complaint they hear is that "the police just don't care." It is important to communicate to the victim that the police do care and for police to be constantly reminded that victims of identity theft often have been repeatedly victimised, that identity theft is an emotionally abusive crime. In responding to the victim's request for a report or investigation of the offence, police are urged to adopt the victim as a partner. Anecdotal evidence suggests that victims are a major source of information about the investigation, both in terms of the financial records that may need to be accessed by the investigator, and in terms of developing a list of possible suspects (Newman and McNally, 2005).

However, researchers believe that studies have shown that several barriers exist concerning communication. How police may react throughout the process of communication may perhaps send out an ambiguous message to the victim. As such, victims of ID theft may feel helpless in cases where they assume that the police's reaction to their report is not satisfactory and therefore, it remains the police duty to ensure that the victims are under no circumstances made to feel guilty of the offence (SABRIC, 2020).

Acknowledging the Crisis (Credit card fraud) Response Plan

According to Andrea, Olivier, Yann, Serge and Gianluca (2014) explained that if a major theft of an agency's database of customer or employee records occurs, the business or agency must have in place a crisis response plan that will minimise the effects on potential victims. Such a plan would usually include: Toll-free dedicated phone lines for employees to call the three major credit bureaus to warn of the theft; and information packets should be distributed to potential victims on what to do, to protect their identities, and to reduce damage. Newman, and McNally (2005). In the researchers’ views, this plan can only be effective if the concerned businesses have the records of their consumers' identifying documents on their systems and provided, such systems are consistently monitored. This may assist in determining the time, location of the suspects, and further help in apprehending the offenders.

Associated challenges of forensic technology in responding to credit card fraud

Expertise about techniques to identify and detect perpetrators using technological and conventional methods, and care for the victims and prosecute the perpetrators of credit card fraud is yet to be realised in South Africa. Reports of the arrests and convictions of the perpetrators of credit card fraud are frequent yet not from the CJS. The implications based on the findings on credit card fraud in South Africa are compelling and require concerted effort from all relevant stakeholders within the CJS. Though the SAPS due to competing priorities, has not yet codify this crime for consumption by the public, it is essential that the official statistics made known to the public. Comparing the number of prosecutions with the number of identified victims would highlight the extent of the problem. The release of official statistics, though argued as unreliable, would nevertheless, provide as an awareness regarding the MO utilised by perpetrators, reported/detected cases in relation to conviction rate to the prospective victims and the public. This would assist all role-players, to develop minimum standards especially technological and conventional methods concerning the response of CJS to trafficking cases as well as improved services to the victims. It is very clear that the victims of this scourge experience psychological and emotional trauma, to the economic and political implications of unabated crime, the impact on individuals and society is clearly destructive and unacceptable.

A lack of role clarity from the relevant role-players related to servicing victims, and uncertainty regarding what measures work and what do not have contributed to a lack of systematic and consistent implementation, and sustainable action. Each calls for different dynamics in policy and programme planning. Lack of utilising technological and conventional methods when dealing with credit card fraud has contributed and acted as an impediment for the SAPS to successfully investigate, combat and arrest the perpetrators of this crime. Lack of skills and training in technology by the SAPS contribute immensely in making this crime uncontrollable and ungovernable in South Africa. An improved cohesion between relevant role-players, would go a long way to align the day-to-day tactics into a long term anti-trafficking strategies and national responses, sharing from their own experiences and identifying elements that constitute best practices.

The MO utilised by criminal involve high skills on technology and very sophisticated measures are applied which can be difficult for third parties to understand, while victims can find it difficult to comprehend what has happened to them, or to discuss it with or explain it to others. Victims may appear to those around them, even support persons, to be uncooperative, irritable, hostile, aggressive or ungrateful. The stigma attached to the victims has a significant and ongoing impact on their lives, including in the trauma experienced as well as the possibility of depression and being in deep debts. The long-term consequences of credit card fraud for victims are complex and depend on many factors, with no guarantee of recovery. Re-victimisation is often a further consequence of the experience.

Theoretical framework: Rational choice theory

It was only during the late 1970s that criminologists realised that none of the theoretical perspectives aimed at explaining criminal behaviour assumed a rational, thinking individual. David Matza’s drift theory (1964) got the closest to including such criteria. He referred to his theory as “soft determinism” However, his theory did not convey the fact that the individual has a free will and that he or she can make a calculated, rational decision or choice.
Theorists, who support the rational choice perspective, speak in terms of “opportunity”, “benefits” and “costs” when discussing the offender’s decision to commit a crime. The viewpoints of Smit (1723–1790), and Bentham (1748–1832) that man exercises economic choices and is motivated to experience pleasure and to avoid pain, featured very strongly in the rational choice perspective. Clark and Felson (1993) indicated that a synthesis of the work of various researchers on criminal decision-making (which fell within four separate disciplines – the sociology of deviance, environmental criminology, economics and cognitive psychology) eventually gave rise to the rational choice perspective of Cornish and Clarke in 1986 (Bezuidenhout, 2011:127).

Instead of emphasising the differences between criminals and non-criminals, the rational choice perspective stresses some of the similarities between them. Cornish and Clark (1986:vii), state that if crimes are the result of rational choices, based on the anticipated cost and benefits, criminal behaviour becomes more crime-specific. They argue that more attention should be paid to the criminal event itself as well as the background or historical and situational factors that influence its commission. This supposes that the decision-making process can be affected by various factors of which situational factors (poverty, unemployment, poor economies and social circumstances) are the most important part of the process in deciding to commit crime.

Therefore, with reference to the above, the rational choice theory states that most opportunistic criminals are rational in their decision making and recognise, evaluate, and respond to a variety of environmental factors (Cozens, 2011:486). These are environmental factors within the built environment which relate to the perceived risk and efforts associated with an offence, and are central to the offender’s decision-making process. The same goes for perpetrators of corruption, they are rational in their decision, and they evaluate and respond to a variety of environment factors, laws, and legislations. The perpetrators of corruption assess where they are going to commit corruption, how they will go about it without raising lot problems.

Research

Qualitative descriptive methodology

This study was exploratory in nature; a purposive sampling method was used following a qualitative descriptive methodology. Thirty-nine interviews were conducted to solicit the views of the participants and police investigators from Vanderbijlpark, Sebokeng, Sharpeville and Vereeniging police stations, members of the community, and victims of credit card fraud were interviewed. The interviews were analysed according to the phenomenological approach, coupled with inductive TCA to identify the participants’ responses and related themes. The reason for this choice was to identify key or knowledgeable participants about credit card fraud in the Vaal Region.

Overall, 39 participants formed part of this study. About 28 participants were purposively selected comprising of the SAPS Constables, Sergeants, Warrant officers, and Captains. Of these, eight were females and 20 males. Their experiences ranged between 10 years to 27 years. The remaining number of participants were two victims of credit card fraud, which were selected using snowball sampling and the convenience sampling was adopted to select seven members of the public from Sebokeng, Vanderbijlpark and Sharpeville. The perceptions, beliefs, and experiences of participants were collected using interview guides with open-ended questions by the first and second authors of this paper. The in-depth interviews were semi-structured, and a more relaxed, informal interviewing method was adopted for rapport and trust building. The interviews lasted for 60 to 90 minutes.

The Focus Group Discussions (FGDs) were conducted with 19 participants to gain new insights but also to triangulate information collected during the interviews in order to increase validity. Both interviews and the FGD were conducted privately at the safe place as agreed between the participants and the authors. A voice recorder was used to record information during the interviews and FGD. The in-depth interviews and FGD were conducted in the local languages spoken in Gauteng Province (IsiZulu, English and Sesotho) and later translated into English. The Key Informant Interviews (KIIs) were also utilised during data collection and 12 participants formed part of the KII. Translator for other official languages was available but none of the participants felt the need, as they were comfortable in expressing themselves in English. The English translation process focused more on getting relevant meaning than exact translations of the verbal information received.

All interviews were transcribed and then studied several times in conjunction with the corresponding non-verbal clues given by the participants using the stated inductive TCA. Field notes provided further guidance during the data-analysis process, supporting the process of dividing the data into identifiable themes. During the process, the results were verified continuously by means of audio and visual recordings of the interviews, which proved very helpful as a means of ensuring data quality. This also provided the opportunity to follow a process by which the different themes could be compared and relations between the different themes could be studied, so as to become aware of patterns that could be categorised. A summary of the main data categories and the sub-categories is presented in the form of themes. Two processes were followed to ensure effective data control. Firstly, all questions asked were written down and then studied several times.

Secondly, data results were compared with existing literature, to identify similarities or discrepancies that might call for further research in future. In addition, field notes that were also written down provided further guidance during the data-analysis process, supporting the process of dividing the data into identifiable themes.
Findings and Discussion

The SAPS challenges of forensic technology in responding to credit card fraud

The participants from the SAPS in all three areas clearly indicated that they do not have technological resources and skills to respond to credit card fraud. They explained that no training on technological tools or any resources at their disposal to deal with credit card fraud. The following were some of their responses quoted verbatim, and no corrections of their language were made:

There is no proper training in the SAPS to deal with credit card fraud, I for example since I joined the SAPS I never went for training especially on using technology in responding or dealing with credit card fraud (Participant 19).

We just open the case for insurance purposes, no technology or proper resources to investigate credit card fraud, it’s a very difficult crime to deal with if you have no resources, skills and technological tools (Participant 12).

No resources at our disposal to deal with credit card fraud, we do not go for training and the criminals use sophisticated methods and ways to commit this type of crime and we do not have skills and resources (Participant 14)

Strategies to combat credit card fraud

The participants from the SAPS in all three areas clearly indicated that they do not have a strategy to investigate credit card fraud as the perpetrators of this crime use advanced technological techniques and tools. They highlighted that they do not have skills, technological tools and they lack resources to investigate cases of credit card fraud. The following were some of their responses quoted verbatim, and no corrections of their language were made:

The SAPS do not have the resources to deal or investigate the cases of credit card fraud. The suspects use technology to commit this crime and they have advanced skills which we don’t have, we don’t attend workshops or extra training with regards to deal or investigate this crime (Participant 4)

I have fifteen years in the police, and I started investigating the cases of credit card fraud eight years ago, I don’t remember myself going to the training or workshop on how to investigate specifically credit card fraud. So there is no strategy that I can say SAPS have in place or we have a booklet that we use to or follow to investigate (Participant 5)

Well, we do not have a proper strategy that we are using or following, as the investigating officers in SAPS we just help each other when it comes to this crime but most of the time, we don’t solve the majority of credit card fraud cases because we really do not have resources to trace the perpetrators, we also lack the skills to investigate this crime (Participant 6)

Modus Operandi of perpetrators of credit card fraud in the Vaal Region

It should be noted that findings such as those given below were similar among all the selected participants, regardless of the study location. Examples of some of the remarks regarding their experiences in terms of dealing with cases of credit card fraud were similar. The participants, when asked about the MO of perpetrators of credit card fraud in Sebokeng, Sharpeville and Vanderbijlpark, explained that perpetrators use advanced technological tools to commit this crime and to confuse the victims as well as the role-players involved in dealing with this crime. They emphasised that the perpetrators use fake cards, technological tools at the Automated Teller Machines (ATMs), work with bank officials to get information of the potential targets. These are some of the responses from the participants (related verbatim):

Copying a credit card and somehow getting hold of the secret pin of the user. Vendors charging more money from the user’s credit card compared to what they have agreed to and without the latter being aware of the charged money (Participant 11)

The perpetrators in most instances try by all means to look for the pin of the user, it can be in the ATM, at the shopping malls when users pay, it can be in the garage when the user pay for the fuel of their car. (Participant 15)

I know a guy who works at one of the garages here in Sebokeng who works with the perpetrators of credit card fraud, he watches the pin of the users as they pay for the fuel of their cars and also the perpetrators use him to clone credit cards”. This is a serious network, it involves people who works in the bank, they help the perpetrators by identifying those clients with lot of money and the perpetrators monitor their lifestyle, what they do where do they buy and the bank officials also provide the perpetrators with the residential address of the potential victims. (Participant 19).

The perpetrators after stealing or cloning the credit card, for them to use money in those credit cards they work with the owners of the designer clothes or clubs to buy alcohol (Participant 30)

The perpetrators use the stolen or cloned credit cards in the designer clothes shops or clubs, they work with shop owners or club. They buy alcohol and spend on it. For example, this is how they do it, they go to the night club swipe the stolen or cloned credit card, maybe they use R50 000 over a weekend there and the owner of club will give them R30 000 back, they swipe R50 000 without taking any alcohol. That means the owner of the club is going to get R20 000. The perpetrators carry lot of credit cards with them wherever they are and we know this people who terrorise the communities but we can’t talk because they work with the police, so we are scared that they victimise us or target us. (Participant 22)
The perpetrators put the chips in the ATM’s which makes the credit card not to come out, then after the victim leave the ATM then perpetrators go to the ATM and get the credit card (Participant 21)

In terms of understanding the “Management and implications for policy,” this study reveals that expertise about techniques to detect credit card fraud, investigate and to prosecute perpetrators is yet to be realised in South Africa. Reports of the arrest and conviction of credit card fraud perpetrators are frequent yet not from the CJS. The implications based on the findings on credit card in South Africa are compelling and require concerted effort from all relevant stakeholders within the CJS. Although SAPS, due to competing priorities, has not yet developed the strategies and methods to investigate, identify and solve the cases of credit card fraud, it is essential that the officers dealing with cases of credit card fraud be equipped and capacitated with necessary investigating skills and methods to successfully solve deal with this problem.

It is crucial that the training of SAPS officials include technological tools, methods to detect and investigate cases of credit card fraud. Comparing the number of prosecutions with the number of identified victims would highlight the extent of the problem. The release of official statistics, though argued as unreliable, would nevertheless, provide as an awareness regarding the MO utilised by perpetrators, reported nor detected cases in relation to conviction rate to the prospective victims and the public. This would assist all role-players, to develop minimum standards concerning the response of CJS to credit card fraud cases as well as improved services to the victims especially with regard to insurance claims. From the psychological and emotional trauma, to the economic and political implications of unabated crime, the impact on individuals and society is clearly destructive and unacceptable.

A lack of role clarity from the relevant role-players related to servicing victims, and uncertainty regarding what measures work and what do not have contributed to a lack of systematic and consistent implementation, and sustainable action. Each calls for different dynamics in policy and programme planning. An improved cohesion between relevant role players would go a long way to align the day-to-day tactics into a long-term technological strategies and national responses, sharing from their own experiences and identifying elements that constitute best practices. A multi-disciplinary approach between all role-players will enhance the successful detection, investigation and prosecution of credit card fraud cases.

The MO involved during the credit card fraud can be difficult for third parties to understand, while victims can find it difficult to comprehend what has happened to them, or to discuss it with or explain it to others. Victims may appear to those around them, even support persons, to be stupid or irresponsible. The stigma attached to the victims has a significant and ongoing impact on their lives, including in the financial stress and constraints. The long-term consequences of credit card fraud for victims are complex and depend on many factors, with no guarantee of recovery. Re-victimisation is often a further consequence of the experience. The following emerging themes were identified in this study: (1) The SAPS challenges of forensic technology in responding to credit card fraud (2) MO of perpetrators of credit card fraud, (3) lack of knowledge and skills to investigate credit card fraud, (4) lack of awareness in the region around credit card fraud and (5) lack of resources to deal with credit card fraud.

Emerging themes and implication

This study presents the following emerging themes as discussed herewith:

**Theme 1: The SAPS challenges of forensic technology in responding to credit card fraud**

The participants indicated that they face many challenges when dealing with credit card fraud. The major challenge is lack of knowledge and skills when it comes to technological tools. The SAPS do not use technology when responding or dealing with credit card fraud, and most criminals use sophisticated technology to commit credit card fraud. Lack of resources and training in using technology should be prioritised by the SAPS and CJS as a whole in South Africa.

**Theme 2: Modus operandi of perpetrators of credit card fraud**

When asked about the modus operandi of credit card fraud, the majority of participants highlighted that perpetrators use different methods which are very complex and advanced. The methods that were used by perpetrators among others were to put the chip at the ATM record the information of the victim and with that information perpetrators are able to withdraw money from the bank account of the victim.

**Theme 3: Lack of knowledge and skills to investigate**

The participants highlighted that the SAPS do not have capacity and lack skills to investigate cases of this nature. Many victims of this crime highlighted that they have reported the cases to the SAPS but the cases remained unsolved due to lack of skills. The majority of participants from the SAPS did not shy away that this crime require technology to investigate it and that they do not have technology on their disposal to investigate such cases.

**Theme 4: Lack of awareness in the region around credit card fraud**

Majority of the participants from the community highlighted that they did not know that credit card fraud exists in Vaal until they become victims of it. They explained that majority of the members of the community do not know about this scourge and explained
that believe that many people will still be victims of credit card fraud. The SAPS members explained that they do not conduct awareness campaigns as their budget is very limited.

Theme 5: Lack of resources to deal with credit card fraud

The participants highlighted that the SAPS do not have resources to investigate credit card fraud, even the population from the SAPS explained that they do not have resources. The SAPS open a case just for the purpose of insurance and they know exactly that they cannot solve the cases of credit card fraud.

Conclusion

This study recommends that the Closed-Circuit Television (CCTV) cameras should be made available in the ATM, where incidents of credit card fraud are taking place. In addition, the police be visible in the areas which are most prevalent to credit card fraud. This study recommends that the SAPS members should be taken for regularly training in order for them to be able to properly investigate the cases of credit card fraud. They should be taken to advance training that will enable them to investigate sophisticated cases involving high technology on credit card fraud. The study also recommends that SAPS should conduct regular awareness campaigns to ensure that the communities around Vaal Region are aware of the scourge of credit card fraud. This study also recommend that the SAPS should be capacitated with adequate resources and skills to enable them to be able to investigate credit card fraud.

This study concluded that credit card fraud is very high in the selected areas of Vaal Region, the modus operandi of perpetrators try different tactics to deceive their victims and also to ensure that it is extremely difficult for the SAPS investigate. If the SAPS can join hands with the communities and other stakeholders, this scourge of credit card fraud can be reduced.

Acknowledgement

Author Contributions: Conceptualization, M.M., M.J.T.; Methodology, M.M., M.J.T.; Data Collection, M.M., M.J.T.; Formal Analysis, M.M., M.J.T.; Writing—Original Draft Preparation, M.M., M.J.T.; Writing—Review And Editing, M.M., M.J.T. All authors have read and agreed to the published the final version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References

Bhasin, M. L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. School of Accountancy, University Utara Malaysia. Ecoforum. 5, 2 (9).

Dzomira, S. (2014), Electronic Fraud Risk in the Banking industry, Zimbabwe, Risk, Governance & Control: Financial Markets & Institutions, 4(2), 17-27.

Accenture Analytics Innovation Center (2015), “Protecting the Customer: Fighting Bank Fraud in a New Environment,” available at https://www.accenture.com, 1-9.

Bhasin, M.L. (2012). Audit Committee Scenario and Trends in a Developing Country, School of Doctoral Studies European Union Journal, 4, 53-70.

Bhasin, M. L. (2013). Corporate Governance and Forensic Accountant: An Exploratory Study, Journal of Accounting, Business and Management, October, 20(2), 55-75.

Bhasin, M.L. (2013a). An Empirical Investigation of the Relevant Skills of Forensic Accountants: Experience of a Developing Economy, European Journal of Accounting, Auditing and Finance Research, 1(2), June, 11-52.

Bhasin, M.L. (2013b). Audit Committee Scenario & Trends: Evidence from an Asian Country, European Journal of Business and Social Sciences, 1(11), February, 1-23.

Bhasin, M.L. (2013c), “Corporate Accounting Fraud: A Case Study of Satyam Computers Limited, Open Journal of Accounting, 2(4), April, 26-38.

Andrea, D. P., Olivier, C., Yann, B., Serge, W., & Gianluca, B. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. Expert Systems with Applications, 41(1), 4915–4928. https://doi.org/10.1016/j.eswa.2014.02.026

Delalmaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: A review. Banks and Bank Systems, 4(2), 57–68.

Ishu, T. M., & Mrigya, M. (2016). Credit card fraud detection. International Journal of Advanced Research in Computer and Communication Engineering, 5, 2278–1021.

Johannes, J., Granitzer, M., Konstantin, Z., & Sylvie, C. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100(2), 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

Payment Association South Africa [Online]. (2016). Card fraud 2016: Protect your card and information at all times. Retrieved July 18, 2019, from https://www.sabric.co.za/media/1038/2016-card-fraud-booklet.pdf
Premium, B. L. (2018) Bank card fraud climbing towards R800-million. 29 April, BusinessLive [Online]. Retrieved September 01, 2020, from https://www.businesslive.co.za/bt/money/2018-04-28-bank-card-fraud-climbing-towards-r800-million

South African Banking Risk Information Centre. (2017). SABRIC digital banking crime statistics. Retrieved August 18, 2020, from https://www.icfp.co.za/article/sabric-digital-banking-crime-statistics.html

South African Banking Risk Information Centre. (2019). SABRIC digital banking crime statistics. Retrieved August 18, 2020, from https://www.icfp.co.za/article/sabric-digital-banking-crime-statistics.html

South African Banking Risk Information Centre. (2020). These are the most common banking scams in South Africa. 27 June, BusinessTech [Online]. Retrieved September 09, 2020, from https://businesstech.co.za/news/banking/409869/these-are-the-most-common-banking-scams-in-south-africa

Publisher’s Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2022 by the authors. Licensee SSBFNET, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

International Journal of Research in Business and Social Science (2147-4478) by SSBFNET is licensed under a Creative Commons Attribution 4.0 International License.