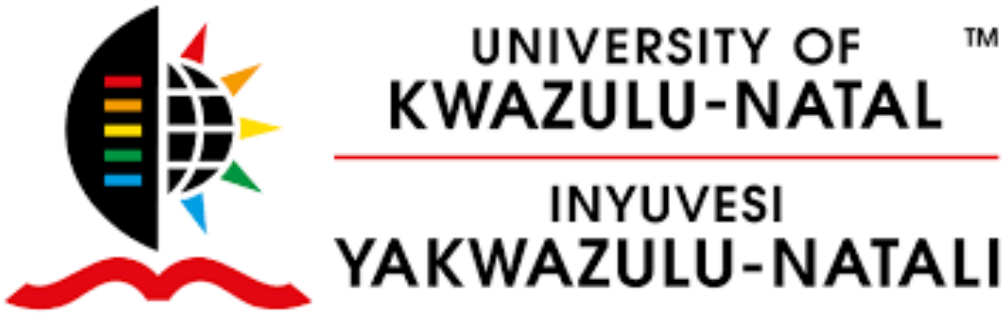
UNIVERSITY OF KWAZULU-NATAL

FACULTY OF HUMANITIES AND SOCIAL SCIENCES



School of Applied Human Sciences

AN INVESTIGATIVE STUDY OF THE POLICING OF IDENTITY THEFT AND FRAUD: A CASE OF THE DURBAN SOUTH AFRICAN POLICE SERVICES SERIOUS COMMERICIAL CRIME UNIT.

by

Fudumezile Lindokuhle Kheswa

Submitted in partial fulfillment of the Requirements for the degree.

Masters of Social Science in Criminology and Forensic Studies

Supervised by: Dr. Londeka Princess Ngubane

July 2021

DECLARATION

I, Fudumezile Lindokuhle Kheswa, hereby declare that the work submitted is entirely my own, unless where acknowledgement indicates otherwise and that no part of this work has been previously submitted for a degree at any other University. The references used have been acknowledged and cited.

Signature of Candidate: Date:

07/07/2021

Fudumezile Lindokuhle kheswa

DEDICATION

This thesis is dedicated to all victims of identity theft and fraud, who are working towards gaining their identity back.

To the young and elderly who are vulnerable to identity theft and fraud.

ACKNOWLEDGMENTS

First and foremost, I want to thank my Heavenly Father whom I could never relay enough gratitude towards, for always being my light and strength throughout my academic endeavors.

My academic journey has always been inspired by family. I know God as my Anchor because of the teachings instilled by my parents. To my father whom never fails to preach the importance of education; thank you for being a mirror upon which my footsteps have always and will continue to strive to reflect. To my mother: your patience, humility and gentleness in all that you do is heartwarming and an inspiration I hope to carry with me forever. I thank you both for the Unconditional love and for never depriving me the means to pursue all that I desire.

To my supervisor who has given me immense support and encouragement. Thank you for the constructive criticism, for always reminding me of my capabilities and strengths when I seemed to have forgotten and overwhelmed. Your words of wisdom and belief have led to the completion of this project. May you continue to exert your intelligence on many others. Soar and Conquer in every aspect of life – *Nyoni Yezwe*.

Linda Coertze, thank you for the relentless time spent editing and perfecting my work. God Bless you!

I would like to express gratitude to the participants who allowed me into their space, shared their experiences and intelligence. Thank you all, for your time and kindness – this project would not have been completed without your assistance.

ABSTRACT

The line between reality and unreality is blurred and, in a postmodern and technologically driven world, it is difficult to tell the real from those things that simulate the real. Extrapolating past events to solve current problems becomes highly risky and often misleading because the strategies employed might not support technological advancement. Against this background, it seems that identity theft and fraud, as separate but also related crimes, are disregarded when criminal phenomena are examined and prioritised. The dangers and disadvantages of this result in little or no fast-tracked plan of action against identity (or ID) theft and fraud. However, it is of great importance to examine ID theft and fraud in depth because of the sophisticated and imminent danger they bring to bear on society. Moreover, these crimes have infamous appeal and their perpetration by criminals worldwide is high due to the unlikelihood of detection. With criminals becoming increasingly adept at both cyberspace and more traditional methods of identity theft perpetration, the criminal justice arena is seen as becoming unequipped and lacking in the ability to keep pace with this form of criminality. The false and misguided belief that only the negligent and careless fall victim to identity theft and fraud should be shifted and the focus should fall on the development of effective and practical solutions to deter and possibly eradicate identity theft and fraud.

It is thus pivotal to explore current processes that drive identity theft and fraud crimes to allow law enforcement to manoeuvre effectively towards deterring these criminal acts. Understanding the tactics and regulatory procedures utilised by law enforcement agencies against identity theft and fraud, and the gaps that might exacerbate these phenomena, is therefore vital in addressing this scourge. Additionally, by comparing and understanding the reasons for current statistics to explain the escalation in these crimes, law enforcement will be able to move towards the design and implementation of new strategies to curb them. The study argues that identity theft and fraud should not be crimes that commercial banks, social media platforms, and internet-based companies are oblivious too. Identity theft exists. It is constantly evolving and causes harm to an increasingly larger group of people, often the elderly, within society. However, the evolution of technology impacts and encourages perpetrators of such criminal behaviour to be more eventful and creative in their approach and modus operandi and enhances their ability to escape and thrive undetected.

The extent of the harm and damage identity theft and fraud cause individuals, families, companies and the government means that their prevalence should never be overlooked or underestimated. The study sought to investigate the policing of identity theft and fraud in the Durban area in KwaZulu-Natal. My examination of these phenomena was not limited to a specific type of identity theft but was all encompassing. The geographical demarcation of the study was restricted to the South African Police Services Serious Commercial Crime Unit (SAPS SCCU), John Ross House, Durban. The goal was to solicit information pertaining to the strategies utilised by law enforcement agencies, particularly the SAPS, to police and deter identity theft and fraud. This was pivotal in light of the rising figures in identity theft and fraud and the lack of research on policing and deterring these criminal phenomena. As one of its main objectives, the study sought to understand the discrepancy between the recorded figures of ID theft and fraud and their actual rates of occurrence. This qualitative study made use of open-ended semi-structured interviews for the elicitation of data to achieve this objective. The study found that various types of identity theft and fraud were perpetrated by syndicates using varying modus operandi, with particular focus on technologically advanced methodologies. What appeared disconcerting was a lack in the ability of law enforcement to keep pace with criminal tactics and the modus operandi utilised by perpetrators that lead to the widespread occurrence of these crime forms. The SAPS SCCU is the only unit that is mandated to investigate commercial crime in KZN, and its success rate, according to the investigating officers, is average to high. However, the capacity of this unit to cope with the workload is somewhat limited due to its geographical jurisdiction that encompasses the whole of the KZN Province. Recommendations are offered in response to the data and the challenges that are associated with the processes of policing identity theft and fraud.

KEY TERMS: Identity theft, identity fraud, policing, investigative research

List of Tables

ACRONYMS

ACRONYM	ABREVIATION
MO	Modus Operandi
SABRIC	South Africa's Banking Risk Information Centre
SAFP	South African Fraud Prevention
SAPS	South African Police Services
SCCU	Serious Commercial Crime Unit
DHA	Department of Home Affairs
ID	Identity Document
Id	Identity
RCT	Rational Choice Theory
RAT	Routine Activity Theory
HIT	Human Identification Theory
KZN	KwaZulu-Natal
POPI	Protection of Personal Information
ECT	Electronic Communications and Transactions Act

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Technology has become ubiquitous in the current era, and being exposed and introduced to its evolving use has granted ruthless individuals inviting opportunities to revert to criminal behaviour (Khuda and Schreuders, 2019:1). This has resulted in some of the most dire consequences for Internet and electronic users at the hands of criminals who look to gain from what was initially meant to be a progressive from of living. Knowledge of extensive safety and security measures in the technological age permits citizens, in one way or the other, to gain a sense of ease and normality in constructing and/or engaging in their day-to-day commercial and financial activities. However, identity theft, in all its forms, deprives individuals of their ability to control as well as govern the events that occur in their lives, and such lucrative information at the hands of criminals means that law-abiding citizens are always at risk.

Identity theft is defined as an "unlawful act of the use of another's personal identifying information" (Bellah, 2001:222). Kahn and Roberds (2008, cited in Dzomira, 2017:1) state that identity theft refers to "the malicious use of personal identifying data". It can also be referred to as the deliberate transfer, possession, or usage of any name or number that identifies another person with the aim of perpetrating or assisting a crime (Kahn and Linares-Zegarra, 2013; Elibirt, 2005; Irfana and Raghurama, 2013). With reference to the aforementioned definitions, identity fraud can then be defined as the stealing and use of another individual's personal identifying information for the perpetration of crime for financial gain. For the purpose of this study, the above definitions of identity theft will be referred to and used interchangeably. As stipulated by a report by the Centre for Victim Research (CVR) that focuses on identity theft and fraud victimisation, identity fraud is a subcategory within identity theft which refers to the use of personal identifying data without the owner's authorisation to do so (Centre for Victim Research, 2019:3). According to CVR (2019:3), it is mostly utilised for financial gain, such as medical identity theft which is the use of the victim's information to receive medical treatment at the cost of the victim. Another purpose such

information may serve is its use by criminals for criminal identity theft, which refers to using personal identifying data to perpetrate a crime such as stealing money from a bank (CVR, 2019:3). As stipulated by Irshad and Soomro (2018:2), "identity theft can be visualized from a number of aspects". One is the traditional method of 'dumpster diving', which is when perpetrators snoop around dumpsters and bins in search of anything they may use pertaining to an individual's personal identifying information that is ultimately used to commit a number of different offenses such as fraud, theft, and cybercrime, amongst others (Irshad and Soomro, 2018:2). According to Irshad and Soomro (2018:2), some perpetrators are known to go through mail that was not shredded before being discarded, while others simply eavesdrop on phone conversations in the hope of catching important information over the phone. These traditional means have now shifted to much more sophisticated methods of identity theft through the use of modern-day information technology.

Identity theft and fraud can be perpetrated using traditional offline methods as well as through cyberspace (Cassim, 2015:2). White and Fisher (2008:2) concur with this view, and stipulate that the methods by which personal information is obtained and subsequently used to commit identity theft are diverse and wide ranging in complexity, ranging from low-tech methods such as theft of wallets or purses and 'dumpster diving', to more sophisticated methods such as internet scams. Identity theft has gradually escalated and is now termed 'cybercrime' (Manap, Rahim, Taji, 2015:1) which occurs in forms such as online identity theft, hacking, and phishing (Khuda and Schreuders, 2019:2). Identity theft has become a gateway for cybercrime as perpetrators can access various cyber platforms using stolen and false identities. Zaeem, Manoharan, Yang and Barber (2017:1) agree with this view. According to Manap et al. (2015:1), the long list of countless advantages that the Internet has opened up over the years has unfortunately been counteracted with the advent and escalation of cybercrime. Irashad and Somonro (2018:1) concur, stating that the various social media platforms that are now enjoyed today due to the evolution of the Internet have also been negatively impacted by criminal behaviour, and by identity theft in particular. Manap et al. (2015:1) further stipulate that, due to the evolving use of technology, "new crimes have emerged and existing ones [have been] exacerbated". The magnitude of identity theft and fraud, and particularly the impact these crimes have on the citizenry, have been difficult to track as suspects impersonate others. This statement is concurred by Cassim (2015:1), who argues that the speed of

technology makes it difficult for law makers to effectively monitor and regulate its use. This dissertation thus identifies and examines technological theft as a hallway for various crimes.

The use of online platforms has been embraced by a large majority of citizens (Jordan, Leskovar and Maric, 2018:1). Below is an illustration of a victim who took to social media to express her rage and frustration after she had been caught up in an unfortunate incident in which she was a victim of identity theft and fraud:

Van Schalkwyk of the SAFPS [cited the] example of a recent case of identity theft and fraud. He reported that a woman had posted on a social media app, Facebook, about a cellular service provider that was supposedly meant to refund her with an amount of R1 500. [This did not occur.] After she had expressed her frustration, a woman then reached out to her posing as an employee of the cellular service provider. The woman [a fraudster] requested the aggrieved lady to send her ID number, payslip, and bank statement to her. In order to ensure that her plans were successful, she [the fraudster] asked the complainant not to speak to any other person(s) from the cellular service company regarding the matter. Soon after she had submitted the requested details, an amount of R15 000 was deposited into her account as opposed to the R1 500 that was owed to her. The perpetrator then requested the aggrieved to keep the R1 500 and send back the balance that had mistakenly been sent to her. The above had occurred twice [before] the complainant discovered that the woman was a fraudster posing as an employee of a cellular service provider. The identity thief had opened several accounts using the disgruntled customer's name and details (Sihlangu, 2019).

According to Sihlangu (2019), SAFPS continues to work with insurance companies, banks, and retail groups to track down and report on new fraud trends in order to eradicate them.

1.2 Background

Cassim (2015:1) states: "Identity theft has become one of the fastest growing white collar crimes in the world". According to Jibril, Kwarteng, Nwaiwu, Appiah-Nimo, Pilik and Chovanciva (2020:2), identity theft is a global pandemic that affects many countries. Its impact is not peculiar to traditional methods of perpetration but spread onto digital platforms. Internationally,

governments and organisations have been confronted with the need to introduce legislation that will lead to strengthening the investigative and prosecutory powers of law enforcement authorities. In many countries, the political and legal spectrum has evolved significantly in order to challenge any risks and/or threats that may confront them, and to counter the ever-changing nature and types of criminal activity that are devised by ruthless scoundrels and syndicates. In the USA, for example, the Identity Theft Penalty Enhancement Act of 2004 was signed into law by former President George Bush on 15 July 2004 (Cassim, 2015:17). Small businesses are the most vulnerable to cyberattacks due to their inability to afford and maintain Information Technology (IT) staff (Bryan, 2020:1). The computer and its various facilities, as well as cellular phones and their derivatives, are commonly used to manage and conduct tasks in businesses and private homes in a more efficient and time-saving manner. It is therefore incumbent for businesses and individuals who access this technology to secure their data.

According to Harrell (2013), in the USA individuals from as young as the age of 16 find themselves victims of identity theft. Those at greatest risk appear to be people aged between 25 and 54 years, as they earn high levels of income and are prone to using cyber technology in its most advanced forms (Vieraitis, 2010: 2). According to Vieraitis (2010: 1) the issue of identity theft internationally, particularly in the USA, has attracted extensive attention. However, in the developing world this has not occurred yet. For instance, it is argued that those mostly targeted by ID theft perpetrators are in the Pacific states where three or more children reside in women-headed households (Vieraitis, 2010: 2). The literature reveals that all affected sectors have taken action against the theft of individuals' identities in the USA and other developed countries, but the same cannot be said about South Africa. In efforts to intensify measures against identity theft in this country, the Identity Theft Enforcement and Restitution Act of 2008 was promulgated (Cassim, 2015:1), but its' successful implementation is questionable.

In India, identity theft is allegedly one of the fastest growing crimes (Cassim, 2015:23). The Indian Computer Emergency Response Team reported 49 455 cybercrime incidences in 2015 alone (Meena, Thomas and Sundaram, 2017:2). On 17 July 2000, the Information Technology Act, also referred to as the ITA Act, was enacted in this country where it is supposed to curb cybercrime and the perpetration of crime in electronic commerce (Rao and Tiwari, 2019:2). According to

Meena, Thomas and Sundaram (2017:3), financial identity theft, which is the use of customers' bank account details and their passwords to commit financial fraud, is responsible for 77% of India's cybercrime.

Jibril et al. (2020:2) stipulates that online identity theft has a dissenting impact in developing countries such as Ghana as opposed to its impact in well developed countries. The reasoning behind this is that the transition of developing countries into the technological and digital world is still relatively young. Concerns have been raised about the inability of developing countries' technological structures to withstand and protect users from online identity theft (Jibril, 2020:2). Ghana was for instance mentioned as one of the top ten countries with a prevalence for cybercrime by the World Bank Survey in 2011 (McCurdy, 2020:6). According to McCurdy (2020:6), this survey included, inter alia, Nigeria, Cameroon and South Africa. African countries have been shown to follow South Africa in their attempts to curb cybercrime, but their efforts have not been highly successful, with Kenya and Zambia sitting at an estimated 61% prevalence rate.

According to McCurdy (2020:8), escalation in Nigeria's economic crime rates dates back to the colonial era. In its effort to combat the scourge of economic crimes such as identity theft after independence, the Nigerian government promulgated the Economic and Financial Crimes Commission Act (EFCC) in 2004. On the strength of this Act, an agency was formed with the mandate to ensure strict enforcement of the EFCC Act in economic and financial crime investigations all around Nigeria, including scrutiny of cases of fraud (McCurdy, 2020:8). McCurdy (2020:9) further states that the work of the EFCC is widely acknowledged and supported by Nigeria's current sitting President, Muhammadu Buhari, the Nigerian legislature, and law enforcement agencies. The rising epidemic of cybercrime also led to the implementation of the Cybercrime Act of 201 in Nigeria, in efforts to deter and combat the misuse of computer and/or electronic device fraud Mohammed, Mohammed, and Solonke, (2019:5 cited in McCurdy, 2020:9). However, many Nigerians hold the perspective that this legislation is inadequate, as offenses need to be proven before perpetrators will be prosecuted. In light of this, lawyers and defence attorneys are thus keen to take on such cases as they are confident that their clients will walk free (McCurdy, 2020:9).

According to Cassim (2015:3), identity theft in South Africa can be traced back to the 1980s when perpetrators obtained victims' identity-related information from a mailbox or by pick-pocketing. In efforts to deter the perpetration of identity theft and fraud against individuals, businesses and government, South Africa promulgated two laws, namely the Protection of Personal Information Act No. 4 of 2013 (also known as the POPI Act) (Cassim 2015:11) and the Electronics Communications and Transactions Act No. 2 of 2002 (or the ECT Act) (Cassim 2015:13). However, Cassim (2015:15) argues that "more stringent penalties are required to deter crafty and sophisticated criminals such as online identity thieves". Brown (2017:1) states that South Africa reportedly lost an estimated R4.5 billion to credit card and debit fraud between 2010 and 2016/2017. With billions of Rand being lost by businesses and private victims of economic crime, an estimated 70% of South Africans have lost all confidence in law enforcement agencies to curb this crime and ensure their safety (Global Economic Crime Survey, 2016:1). This fast growing crime phenomenon within the South African economy has serious implications for all sectors. For instance, South Africa is rated amongst the three top countries in Africa with the fastest increase in cases of fraud through recycled deceased identities (Alfred, 2015). Social media platforms, that form a large part of today's social and economic tapestry, are breached and have become some of the most prevalent sources for the crime of identity theft. This can be largely associated with the lack of security measures to protect users on these platforms. The responsibility of ensuring that personal identifying information remains exclusive is therefore placed on the shoulders of the social media user.

However, legislations have also been signed into effect in order to respond to cases of invasion of privacy and the theft of personal information, yet this has not prevented nor combated the scourge of identity theft, and cases of identity theft and fraud continue to rise despite legislative implementations (Eboibi and Richards, 2019: 23). Manap et al. (2015:2) state that the Internet has granted perpetrators opportunities to operate anywhere in the world and to do so without detection. Although commonly known methods have not been distinct, the Internet has assisted perpetrators in shifting from traditional methods − such as dumpster diving − to more sophisticated means of ID theft such as using information technology (Manap et al., 2015:2).

It is undeniable that commercial crime is a global pandemic that affects not only developing countries, but developed countries as well, and this fact begs the question whether South Africa, and more specifically the SAPS in Durban, KwaZulu-Natal, is ready to employ effective strategies to deter identity theft both conventionally and on digital platforms. It was against this backdrop that the researcher investigated the investigative and policing procedures utilised by the South African Police Services Serious Commercial Crime Unit in her efforts to determine this unit's efficacy in curbing identity theft and fraud.

1.3 Study Justification

"The central importance of research in todays' world is something we take for granted and that we seldom step back and focus on explicitly" (Punch, 2013:4). The remarkable feature of our culture is that research is seen as an effective way of answering questions, solving problems, and developing knowledge. Therefore, the purpose of engaging in this research was to answer certain questions, attempt to solve varying problems about the research problem as identified by the researcher, and to develop and expand knowledge about the research topic, namely ID theft and fraud.

In 2016, a total of R374 million was lost due to credit card fraud (Brown, 2017). Although this amount had decreased from R463 million in 2014, the extent of this loss is not commendable (Brown, 2017). The wide range and depth of identity theft and identity fraud by perpetrators is incomprehensible, and the ability of such ruthless perpetrators who operate either as small-scale fraudsters or large networks extending internationally without detection calls for the assessment of the Hawks' cybercrime unit as well as the SCCU of the SAPS if their operations are to improve drastically. The researcher thus explored the mandate of the SAPS in dealing with both the statutory offenses that relate to legislation under diverse areas, from banking and currency to electronic crimes (EC's), as well as common law offenses that include fraud and theft (Jordaan, 2008:15). Advancements in the methods used to perpetrate ID theft and fraud vary from low to high technology. The growth in the operation of fraudulent conduct has advanced to the extent that data are hacked/stolen off large data bases by syndicates (Ngema, 2017:1).

The results of the study will benefit the scholarly community as the researcher envisions publishing the findings in an accredited journal. The findings of the study will also contribute to organisations and programs that deal with the prevention, detection and investigation (policing) of identity theft. The researcher also hopes to present the findings at conferences that seek to assist the SAPS SCCU to improve their current methods of preventing and investigating the scourge of identity theft.

There is a large discrepancy between cyberspace identity theft and the reality of the world we live in (Manap et al., 2015:2). Cyberspace is constantly evolving and elevating with the introduction of new information technology almost on a daily basis. According to Manap et al. (2015:2), this makes it difficult for law enforcement agencies to maintain their pace or keep up with evolving developments. However, this should not be used as an excuse not to keep up with the current trends and adopting new techniques and investigating procedures to curb and combat new crime. Citizens rely on and look to law enforcement agencies for protection, therefore it should not be perceived that crimes of any kind are impossible to be curbed by protection services. It is this reality, and the rise in the crime of identity theft, that led to the current investigation to determine how such crimes are policed in Durban, KZN.

Some may mistakenly argue that mounting cases of identity theft and fraud only alarm fellow South Africans and thus they do nothing to assist the situation. The researcher thus focused on the Commercial Crime Unit of the SAPS to inquire about their detection and prevention methods and processes in curbing ID theft and fraud. Part of the inquiry also focused on advancements in this unit's methods to investigate both low and high technological perpetration of this form of crime.

1.4 Problem Statement

According to Brown (2017), over the past seven years a total of R1.9 billion has been associated with debit card fraud. Data collected from South Africa's Banking Risk Information Centre (SABRIC), which is an organisation dominated by local banks, have shown that 48% of credit card fraud losses occurred throughout South Africa, while 80% of debit card fraud occurred in the Gauteng Province (Brown, 2017). "Card payments constituted 61% of all payment transactions processed in South Africa in 2016, with more than 60 million debit cards and 8 million credit cards

having been in circulation" (Brown, 2017). Identification fraud, through using credit and debit cards, has been an evolving epidemic in this country. Perpetrators of identity theft generally use the personal information of victims to open bank accounts and to perform account takeovers (Mthukwana, 2019).

Mlamla (2020) stipulates that the Western Cape's capital city, Cape Town, saw an increase of 20.5% in debit and credit card fraud between 2018 and 2019. This increase was attributed to online transactions. In a statement released by the Chief Executive, Nischal Mewalall, of SABRIC on the overall crime statistics for 2019, he stated that it was commendable that a decrease in identity theft and fraud had been noted in Limpopo, Mpumalanga and the Western Cape (Mlamla, 2020). Significant decreases also occurred in the North West, Free State, and the Gauteng provinces (Mlamla, 2020). However, in 2020 unfavourable rates of identity theft and fraud were again recorded. According to Mlamla (2020), Standard Bank's head of digital banking, Andrew van der Hoven, stated that there was a notable increase in April of that year with regards to phishing scams, which is a process whereby perpetrators utilise online platforms such as websites and/or SMSs to lure customers to reveal their personal information. It was reported that companies could experience an increase in cyberattacks, as Bruce Watson of the University of Stellenbosch argued that many cyber-security professionals were working from home amid the COVID-19 pandemic, making it difficult for these professionals to defend their companies against cyberattacks (Mlamla, 2020). Bruce Watson further cautioned fellow civilians, stating that, as many people were working from home, this limited them and encouraged the use of shortcuts as opposed to proper, detailed verification, which increased the risk of cybercrime.

Contrary to the aforementioned dilemma, the pandemic seemed to fast-track the use of technology and online platforms during the pandemic (2020/2021). In the Western Cape, increases in identity theft escalated again at the end of 2020 (Magoma 2020). According to Magoma (2020), this escalation sparked the interest of many organisations that then took the initiative to look into the prevalence of identity theft and the impact it had on victims. Magoma (2020) further postulates that many victims are unaware that they have been victimised, as they only notice the impact when they apply, for example, for a loan to buy a car or a home, or when they check their credit score. Financial fraud is becoming a trend in South Africa with many citizens of the Western Cape

Province indicating evidence of unusual and fraudulent transactions from their accounts (Magoma, 2020). Such incidences leave victims with a negative financial record and the possibility of being blacklisted. “There has also been a number of people who have been blacklisted over unpaid accounts they’ve never opened or unpaid invoices from reputable companies that they have never engaged with” (Magoma, 2020). The reason for such incidences is that companies and organisations permit people to register, open accounts, and agree to contracts telephonically without being physically present to submit vital documentation which would ensure authenticity and allow for verification of identity. Fraudsters thus take advantage of such non-contact opportunities and rely on the gullibility of law-abiding citizens by opening accounts and making purchases using stolen information belonging to these victims (Magoma, 2020).

According to the South African Banking Risk Information Centre (SABRIC), the worst form of card fraud transpires when credit and debit card fraud is committed in the absence of an actual physical card, which is known as a ‘card not present’ (CNP) loss. In this case a credit card number is obtained and (Brown, 2017). The Chief Executive of SABRIC stated that CNP was the most common form of identity theft and fraud, with perpetrators of this crime often executing transactions in foreign countries while the card is in the victim’s possession (Mlamla, 2020). In 2018/2019, an increase of 99% in such fraudulent transactions occurred (Sihlangu, 2019). The researcher focused on such crimes in Durban Central, KZN, where a high commercial crime rate occurred 2012, decreased in the three years thereafter, and increased yet again in 2016. Mthukwana (2019) of the *Sunday Times* reported that the Executive Director of the Southern African Fraud Prevention Service (SAFPS), Manie van Schalkwyk, postulated that identity theft would double each year after 2019 as provinces such as KZN and the Western Cape had experienced a “double digit increase in commercial crimes”, with KZN at 16% and Western Cape at 11%.

In most instances, victims are blamed and accused of negligence when such crimes occur. This is particularly incomprehensible as overseers are appointed to ensure the prevention and detection of such crimes. Dzomira (2017:2) argues that financial organisations should be blamed as they should take the necessary steps to educate their clients, particularly in developing countries where many may be illiterate. Thus, if they these companies do not take any appropriate steps, citizens may find themselves on the receiving end of identity theft (Granova and Elof, 2004; Dzomira, 2017:2).

It is due to some alarming statistics, such as those mentioned earlier, upon which the researcher decided to investigate the policing of identity theft and fraud within the Durban Central region in KZN. The call for the researcher to specifically focus on identity theft and identity fraud was enhanced by the prevalence of these crimes in this area, as was revealed by the Global Economic Crime Survey (2016:9).

1.5 Identity Theft: Definitions

McNabb (2015:31) points out that a problem is usually conceptualised using a set of concepts that have been identified and acknowledged by the researcher. These concepts are then examined as variables that are explored and become pivotal in a study (McNabb, 2015:31).

1.5.1 Definition of terms

According to Strouple and Archer (2007:1), "it is essential for researchers to provide an acceptable definition of the subject of their work in order for results to be accepted and communicated to the academic community and ultimately to the community at large". In order to better understand the term identity theft, the researcher will define identity, theft, and fraud separately and further explain these terms in a conjoining manner. The following key terms are defined for the purpose of this study: policing, investigative research, theft, identity theft, online identity theft, and identity fraud.

Manning (2010:3) defines ***policing*** as follows: "Policing is about the management of uncertainties and rests on compliance and mutual trust. It fits well with the notion of high modernity in which strategies must interact repeatedly in some civilized manner." An example of the ***act of policing*** is described as: "Keeping law and order in an area, [and] ensuring that a particular set of rules is obeyed" (Oxford Dictionary, 2015:687).

Ladyer (2018:3) describes ***investigative research*** as follows: "Investigative research offers an alternative approach to social science research. It can be used to explain social behavior in any empirical area. However, as with data samples, research problems are not rigidly 'determined' in

advance. Rather, they are 'explored' theoretically and empirically during research ... that is exploratory in nature or character in a sense of being open to possible outcomes, regardless of the amount of previous research on the area or problem". The researcher must thus be ready to view a phenomenon from various perspectives and angles.

According to Golladay and Holtfreter (2017:3), ***theft*** can be defined as: "The unlawful taking of information (for example, personal account numbers or even tangible items such as credit cards or checkbooks)". ***Identity theft:*** Generally, identity theft refers to the stealing of the above traits and or characteristics for the purpose of committing fraudulent activities. According Khan and Zegarra (2016:8), identity theft is "the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime".

Wang, Zhang, Li and Zong (2019:2) define ***identity fraud*** as follows: "[It is] one person using another's personal information or combining a few pieces of real data with bogus information to deceive a third person". Ahmend (2020:50) argues that identify fraud is: "...any event that occurs when a false identity is used, or when another individual's details are used in support of illegal activity, or when a person avoids obligation or liability by falsely claiming status as an identity fraud victim".

Although there are various definitions for ***online identity fraud,*** for this study the definition by Jordan et al. (2018:2) was the most suitable:
"...online fraud describes crime that involve[s] the duplication of digital information or the hi-jacking of online accounts for the purpose of committing identity fraud against individuals or businesses".

1.6 Aim and Purpose of the Study

The aim of the study was to investigate current strategies utilised by the Commercial Crime Unit of the SAPS to determine if it was successful in investigating and deterring identity theft and fraud. The purpose was this to gain in-depth understanding of the observed discrepancy between the figures reported and recorded for identity theft and fraud and the policing and procedural strategies

followed by Serious Commercial Crime Unit of the SAPS. Furthermore, the researcher aimed to gain an understanding of the realities faced by this unit in dealing with cases of this crime. By utilising the knowledge gained through this study, the researcher hoped to raise awareness and contribute to the body of knowledge that already existed in this field of academia. The researcher also wished to assist in alerting protective services to some of the hardships faced by victims of the crime of ID theft and fraud and, simultaneously, to aid them in creating constructive and productive strategies that will be successful in deterring these crimes.

1.7 Study Objectives

The primary purpose for social science research is to examine and understand the motivation and truth that drive human behaviour and to obtain intimate background and knowledge of society and its functioning (Girija, 2003:3). After careful review and consideration of the existing literature and statistics concerning identity theft and fraud, the following research objectives were devised:

- To assess the nature of identity theft in Durban;
- To investigate the causes of identity theft in Durban;
- To examine the effectiveness of the strategies employed by the SAPS CCU in policing identity theft in Durban;
- To identify the challenges experienced by the CCU in policing identity theft in Durban; and
- To recommend strategies to curb identity theft in Durban.

Each objective will be clarified in more detail.

One: To assess the nature of identity theft in Durban

The Global Economic Survey (GES) points out that no sector or region is immune to economic or commercial crime. Advancements in the methods utilised by identity fraud perpetrators and syndicates have rendered many organisations and businesses victims of economic crimes in South Africa (GES, 2016:2). A perusal of the literature made it clear that KZN was taking the lead in credit card fraud, particularly because of the resourcefulness and sophistication of identity theft perpetrators in this region. It was also revealed that it had become very difficult to ascertain which

type of identity theft was the highest. It was also evident that, thus far, not much research on identity theft had been conducted in South Africa, particularly in Durban, KZN, regardless of the fact that it had the highest figures of commercial crime among the nine provinces (Statistics SA, 2017:2).

Two: To investigate the causes of identity theft in Durban

The literature revealed that the inattentiveness exhibited by retailer businesses, banks, cell phone stores and travel agencies was the most disquieting contributor to identity theft. What was evident was that these agencies tended to discard clients' personal information carelessly, thus making it easy for ID theft perpetrators to find and use this information to their advantage (Cassim, 2015:9). This, however, only explains *how* an individual is victimised, and not *what causes* identity theft and fraud by perpetrators. As a Criminology researcher, it was thus important that the researcher addressed what and why questions of these phenomena in a scholarly investigation. Part and parcel of the criminologist's focus is to examine and study the criminal mind and explore the causes of a crime. Therefore, this objective was devised to gain an understanding of identity theft and to possibly to find a strategy for combating this scourge in society.

Three: To examine the effectiveness of the strategies employed by SAPS SCCU in policing identity theft in Durban

According to Cassim (2015:10), identity theft is embodied in the common law, meaning that person(s) guilty of identity theft may be prosecuted for fraud, forgery, and uttering a forged document, each of which is dependent on the specific case. Sentences for the above offenses range from a minimum of 15 to a maximum of 25 years' imprisonment, with sentences imposed as per the Criminal Law Amendment Act No. 105 of 1997 (Republic of South Africa, 1997) (Cassim, 2015). Identity theft is escalating regardless of the existence of this law, and it was thus pivotal to examine the strategies utilised by the SAPS CCU to determine its' effectiveness in apprehending and convicting perpetrators of this law.

Four: To identify the challenges experienced by the CCU in policing identity theft in Durban

Statistics South Africa (2017:2) revealed that, at the time, 32% of South African organisations had reported being victims of cybercrime. As billions of Rand are lost annually by businesses and

many other victims of economic crimes, an estimated 70% of South Africans have lost all confidence in law enforcement agencies (Global Economic Survey, 2016). It was thus important to examine the challenges experienced by the special crime unit to understand the incline in the numbers recorded for ID theft and fraud.

Five: To recommend strategies to curb identity theft in Durban

It is comforting that various bodies service victims of identity theft in South Africa and that, despite the prevalence of this crime, many organisations are now taking the initiative to protect potential victims and to combat identity theft. According to Magoma (2020), Cape Town's provincial government has made it their responsibility to educate the public on how to protect themselves against the perpetrators of identity theft. However, although commendable, the figures surrounding this epidemic are still far too high for South Africans to be at ease, and this is particularly true for KZN (Mlamla, 2020). The figures insinuate that current strategies are inadequate, and therefore new practical solutions and plans must be initiated and implemented. It was thus of great importance to consider the views of the research participants as it was envisaged that they would assist in suggesting new strategies that would be of great interest to the researcher.

1.8 Key Research Questions

Bryman (2015:7) stipulates that a research question is "a question that provides an explicit statement of what it is the researcher intends to accomplish by conducting the particular study". Therefore, in light of the preceding objectives, this study was guided by the following research questions:

- What is the nature of identity theft in KZN Province?
- How effective are the strategies utilised by the KZN Province in policing identity theft?
- What challenges do the SAPS CCU face in their efforts to police identity theft in KZN Province?
- What actions can be taken to remedy the challenges experienced in policing identity theft in KZN Province?

1.9 Methodology

"Research methodology is known as a way of thinking about and studying social reality" (Strauss and Corbin, 1998:1). It is pivotal for the researcher to ensure that they select the appropriate and fitting way of thinking and looking at the phenomena understudy. For this study, a stance of an Interpretivist Paradigm was assumed. The study is further motivated by the Phenomenological Approach through its' basis of inquiring and soliciting the lived experiences and expressions against social phenomena such as crime (Johnson and Parry, 2016:49). Upon consideration of the premise of the study, fit for collection of data was the adoption of a Qualitative Approach, which allowed for the attainment of rich and detailed information regarding ID Theft and Fraud. Participants were selected using Purposive Sampling and Snowball Sampling techniques. The study was conducted with the SAPS SCCU located at the John Ross House, Durban. The researcher made use of both primary and secondary data, attaining information through the use of open ended semi-structured interview questions and secondary data by accessing the Malherbe Library at the University of KwaZulu-Natal. A total of 12 participants were interviewed. To analyze the data, the researcher made use of thematic analysis and was assisted by the NVIVO software to manage and sift through relevant data. A more detailed description of the methodology used to be discussed later (see Chapter 3).

1.10 Study Progression

Chapter One: **Introduction**

This chapter serves as the introduction to the research study. The researcher discusses the background to the study topic, followed by the problem statement, the research objectives, and the research questions. The structure of the research dissertation is also presented.

Chapter Two: **Literature Review**

This chapter presents an in depth deliberation on identity theft and fraud. A brief history is provided and the different types of identity theft and fraud are listed Each objective is discussed in consultation with existing literature.

Chapter Three: Theoretical Framework

This chapter is an overview of three different theories that were used in the study. The rational choice theory (RCT) was employed to understand the criminal behaviour of identity theft and fraud perpetrators. The second theory, namely the routine activities theory (RAT), was used to explain how people might fall victim to identity theft and fraud. Lastly, the human identification theory, as propagated by Professor Roger Clarke, was used to explain what features and characteristics could be focused on to manage and prevent ID theft and fraud.

Chapter Four: Research Methodology

This chapter expounds the research procedures that were employed in this study. The researcher explains why the qualitative research approach was adopted and describe the data collection tools. The NVIVO approach that was used to organise data is discussed and the thematic data analysis method that was used is explained.

Chapter Five: **Data Analysis**

This chapter describes the data analysis process using thematic analysis. The NVIVO software is again referred to and the researcher stipulates the ways in which the software assisted in organising data. The process of coding and identifying themes using thematic analysis is clarified in this chapter. The themes are then discussed in relation to relevant literature findings while the theories that were selected are used to underpin the findings based on the data.

Chapter Six: Recommendations and Conclusions

The five objectives of the study are discussed and reviewed in relation to the collected data. Each objective is explained in regards to whether the aim of the objective was achieved. Recommendations are made per theme and in terms of the challenges identified in the study. Conclusions or short summaries of each chapter are offered in relation to the study. The discourse is concluded with pertinent remarks about the study as a whole.

1.11 Conclusion

This was an introductory chapter that provided the background to the study, with particular attention to the criminal phenomena of identity theft and fraud. The aim of the study was clarified and the objectives and research questions were clearly stipulated. The chapter thus provided an overview of what the study entailed and highlighted key elements in the literature that will be discussed in greater depth in the chapter that follows.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The following chapter examines historic and present understandings of what is known and surmised about identity theft. The review focuses on South Africa, but the discourse also addresses and acknowledges literature on identity theft from the United States, India, and the United Kingdom.

2.2 Nature and Extent of Identity Theft

2.2.1 Potential victims of identity theft

Various characteristics are taken into consideration when looking at what could possibly make an individual a potential victim. For instance, age, income level, education, number of adults in a household, number of children, gender, marital status, race and ethnicity, and geographic region may be considered. According to Anderson (2005:12), demographics influence the possible victimisation of an individual who is exposed to identity theft. He further stipulates that persons with high levels of income are at great risk of victimisation, while households with one adult are also at high risk of being victims of ID theft. Rodriguez, Ser, Bastida, Bilbao and Sanz (2015:10) state that social network users are the recent most popular target group for identity theft perpetrators. For instance, social media allow the spreading of malicious messages or interacting with an individual's personal identifying information through easier and accessible means, and particularly those who do not enrol in securing options to safeguard their personal information online are at risk of identity theft and/or fraud.

A paper by the US Department of Justice (2012:18) stipulates that identity theft is an equal opportunity crime, meaning that it is not race, age, financial, gender, or ethnicity specific. Rather, anyone may become a victim of this crime. The National Crime Victimization Survey and Federal

Trade Commission state that a high risk of victimisation exists amongst people aged 18 to 24, which suggests that students are more likely to become victims of identity theft than older adults (Holt and Turner, 2012:5). This, of course, does not exclude or downplay the risks associated with any other age group that may also be exposed to this crime. Kempen (2017:2) stipulates that it is important for the ID perpetrator to access the potential victim's personal information, as without such information they are unable to commit fraud. As will later be discussed, potential victims are sourced by making contact with them by telephone, email, bogus internet websites, mail, or in person (Lewis and Tapley, 2009:13). The following resources are often used as lures to target victims:

- Open source directories such as phone books, lists of directors, and lists of shareholders. Such lists are normally available to whoever wishes to use them to contact potential clients. Individuals employed by companies who make such lists available are thus potential victims, or they expose their clients to victimisation.
- Marketing lists (such as known purchasers of lotteries or health products). There are millions of people who engage in both or either of these activities, and targeting and managing to scam them is often not difficult.
- Illicit lists ('suckers', personal information lists). According to Lewis and Tapley (2009:13), fraudsters gain access to people who commonly play the lottery. The 'suckers list' comprises a group of people who were previously scammed. The researcher argues, however, that a previous identity theft victim who was caught in a scam may be less gullible and more vigilant.

The uncontrolled usage of online computer users heightens the chance that potential victims may interact with various people from all over the world, and some may be ruthless ID theft perpetrators who target vulnerable users (Holt and Turner, 2012:5).

2.2.2 Offender typologies

A fundamental question in criminology is "...whether crime requires specialised skills or [whether it] is simply a low-skilled endeavour committed with little thought or planning" (Vieraitis, Copes, Powell, and Pike, 2015:1). According to Newman and McNally (2005:37), offender typologies are

studied and examined according to different crimes, but information is lacking for identity theft perpetrators. This will of course be the case as they assume false identities when committing their crimes and/or fraudulent activities. Most information in the literature regarding the perpetrators of identity theft was derived from interactions with law enforcement officials, surveys, and literature reviews. It is notable that identity thieves use and may be addicted to drugs, particularly methamphetamine (Newman and McNally, 2005:37).

For the purpose of this study, all typologies known and listed for identity theft were included. This is because the study did not focus on a specific type of identity theft, but on the policing of identity theft in general. Newman and McNally (2005:38) make note of two types of offender typologies for identity theft perpetrators, namely low-frequency and high-frequency offenders.

2.2.2.1 ***Low-frequency offenders (novices)***

Newman and McNally (2005:38) stipulate that low-frequency offenders can be briefly defined as perpetrators who do not make use of high technology to commit their crimes and who are commonly individuals who do no ultimately perceive their actions as criminal. However, this is not true for all low-frequency offenders as the can be divided into two types of offenders, namely:

- Crisis responders: As was mentioned before, crisis responders may not all be individuals who perceive their actions as criminal, such as a mother or guardian who open a credit account using her child's name (Newman and McNally, 2005:38). The reason for this action may be that the mother is in debt or may have compromised her credit rating. Another type of low-frequency offender may be a criminal who assumes a new identity due to the fact that there is a warrant out for his arrest. McNally and Newman (2005:38) state that such individuals act on a "perceived crisis" and thus their actions are in response to this perceived crisis.
- Opportunity takers: Contrary to crisis responders who act on a perceived crisis, opportunity takers "respond to the desire to take advantage of some criminal opportunity" (Weisburd, Waring, and Chayet, 2001:64). Newman and McNally (2005:38) make reference to a cashier who takes a customer's credit card that was mistakenly left on the counter. The cashier then uses the credit card to purchase goods. Offenders in this group may also be

those who find a wallet or bag lying around and they then find an ID document or credit card inside the victim's bag. Such offenders use anything they can to make unauthorised purchases or assume the victim's identity.

2.2.2.2 High-frequency offenders (experts)

High-frequency offenders can be described as offenders who use sophisticated means to commit crimes (McNally and Newman, 2005:38). Although they may also seek and make use of criminal opportunities, extensive planning is involved in the execution of these crimes. According to McNally and Newman (2005:38), just like low-frequency offender typology, high-frequency typology is also broken down into two types of offenders, namely opportunity seekers (opportunists) and stereotypical criminals.

- Opportunity Seekers: Offenders in this group seek opportunities that allow them to commit specific crimes (McNally and Newman, 2005:38). For instance, in order to deliberately gain their personal information, hackers create unreliable or fake sites on which they advertise and offer products and services that people are likely to need. McNally and Newman (2005:38) state that offenders such as dumpster divers and scammers are examples of opportunity seeking offenders.
- Stereotypical offenders: According to McNally and Newman (2005:38), these are known as the highest frequency offenders. They have a "mixed bag of criminal conduct, and their personal histories often include a difficult childhood, substance abuse, and other problems" (Weisburd, Waring and Chayet, 2001:83-84). This group is known to work at a high level of sophistication and these people are capable of conducting any form of identity theft.

As important as it is for civilians to know and understand the above types of offenders, it is also pivotal that police officials understand and communicate knowledge of them to all parties who are likely to be affected. Researchers who conduct surveys and may rely on such information should also remain informed by means of scholarly journals, newspaper articles, and other reputable sources. Criminologists in particular should be aware that certain types of crime, particularly ID theft, require extensive skill, time, and planning.

2.2.3 Identity thieves' modus operandi

As there are both high- and low-frequency offenders of identity theft, the manner in which they commit their crimes varies. For the purpose of this study, the researcher will refer to and explain all types. It is argued that there is either a fair amount of or little skill required when committing criminal activities, as most offenders are seen as opportunists and thus it would make sense that not much skill or planning is required (Copes, Powell and Pike, 2015:3). Mainly two types of methods are utilised by identity theft syndicates, as explained by Copes, Powell and Pike (2015:3) and other scholars.

2.2.3.1 Low-technology ID theft

- This refers to offline methods of stealing and gaining information from victims. Low technology crime rates in this field remain relatively high as little skill and limited planning are required. For instance, any person may snatch and grab an individual's wallet or find a bag and see this as an opportunity to commit a crime using the victim's personal information. Leukfeldt, Kleemans and Sol (2016:1) state that this group of offenders is known to operate locally and internationally.
- Offenders obtain information through businesses or institutions that store customer, employee, as well as student records.
- A useful piece of information for perpetrators is a victim's social security number (or ID number in South Africa) which assists them in acquiring or revealing the victim's personal information. ID numbers are commonly utilised by different facilities such as banks, policy/insurance companies, and higher education institutions.
- Some perpetrators go as far as posing as employment agencies and conduct interviews. In this manner they obtain victims' personal information.
- In hi-tech criminal instances, some criminals set up fake employment sites to gain access to victims' personal information.
- Person(s) working at call centres, banks, car rentals, or insurance companies may be working with an identity theft perpetrator as an 'inside man'. Once the perpetrator has

the victim's identity document, they may contact the employee who will assists them to gain access to a victim's personal information.

- According to Kempen (2016:1), perpetrators are also known to call their victims, for example they pretend to be a bank or insurance company requesting a change of home address. This results in sensitive information becoming available.

2.2.3.2 High-technology ID theft

- According to Allison, Amie, Shuck, and Lersch (2005:1), high technology refers to criminal activities that are conducted skilfully and with expertise. Technology has proven to be an easy and quick way for this as it is particularly known for its little time-consuming trait. Contrary to low-tech offenders, high-tech perpetrators have the means to operate internationally (Leukfeldt, Kleemans, and Sol, 2016:1). The Internet allows individuals to pay their accounts and send their information wherever and to whoever without physically going to the designated facility or institution. As good as the Internet system thus may seem, it has had unfavourable consequences for many users at the hands of high-frequency offenders, particularly those of organised gangs and syndicates.
- According to Copes, Powell and Pike (2015:3), these are well-organised offenders who will operationally plant one of their members in a bank, the Department of Home Affairs, or other pivotal organisations where they readily access sensitive information.
- This group may operate under a type of defraud known as 'individual to business' fraud. These perpetrators will set up for example a fake insurance company where potential employees will relay personal information as part of the application and screening process (Wall, 2013:6). Paramount to these companies is their use of existing known and trusted brands to lure victims, resulting in the exploitation of their identities.
- These syndicates go to the extent of creating what is known as malware which they use to infect different networks. This decreases victim and perpetrator interaction. Should the victim visit or click on the site, their computer is immediately infected with the malware. When the victim withdraws money, as much as half of the money goes to the

perpetrator as programmed by the malware without this fraud being visible to the victim.

- These perpetrators steal victims' bank card information and use it to withdraw money from their accounts. According to Wall (2013:6), they normally work with an individual within the group known as 'money mules' who are sent to withdraw money and are paid a fee for each withdrawal.
- "Warning! The security of your online bank account needs to be updated. Update today or your account will be blocked. Click here to go to our secure website directly." According to Leukfeldt, Kleemans and Sol (2016:3), this is one of the statements used by identity theft syndicates to lure victims. They instil the fear that their accounts will be blocked and victims will than enter these sites by divulging important information to the fraud syndicate.

2.2.4 Types of identity theft

The South African Banking Risk and Information Centre (SABRIC) (2019) is a non-profit organisation that frequently issues the latest information regarding different types of criminal activities. A recent list of the different types of identity theft scams currently in existence was issued, listing the following schemes and/or techniques:

- Social engineering
- Email hacking
- Phishing
- Vishing
- Smishing
- Internet banking
- Cellphone banking
- Card fraud
- ATM fraud
- Classified/Holiday scams
- Debit order scams
- Deposit and refund scams
- Get rich quick scams
- Technical support scams
- Cyber crime
- Changing bank details
- Contactless bank cards

There is a slight difference between high technology and low technology fraud. Although the most common type is low technology, well-organised offenders deal with high technology types which,

in most cases, are likely to attack a large group of people at the same time. What poses a severe danger by this group is their ability to operate without any interaction with the victim, which leaves the victim with no chance of identifying a threat against their accounts or personal information. This is opposed to a regular thief targeting and stealing a purse off a single victim. With low technology crime remaining relatively high, hi-tech identity theft syndicates are advancing their methods of conning and scamming people.

The above list of identity theft crimes indicates new and highly technological skills. The list also suggests that identity theft perpetrators are constantly developing new modus operandi to make it increasingly difficult for security systems as well as police officials to detect them and for victims to be completely unaware of the trap they are falling into. This requires that police officials remain vigilant and conduct thorough investigations in order to be in constant parallel with the methods utilised by identity theft syndicates. It is important to note this may only happen should victims report being victimised, which will then allow officials or bank systems to conduct investigations.

2.2.5 Steps involved in committing identity theft

The increase in identity theft in South Africa can be attributed to the opening of credit card accounts under false and/or stolen personal identifying information. Such cards are used to run up debts and the claiming of false tax refunds from the South African Revenue Services (SARS). A contributing factor that facilitates this form of fraud is that retailers, banks, cell phone stores and travel agents have been discarding clients' personal information carelessly, thus making it easier for perpetrators of ID fraud to find and use this information to their advantage (Cassim, 2015: 9). Below are the steps that are followed by perpetrators to commit identity theft:

- Obtaining Information: Identity theft perpetrators acquire personal information from their victims in various ways. They do this either by means of high or low technological skills. As was mentioned earlier, a low technology perpetrator will steal a victim's wallet or purse and thus acquire their personal information. The perpetrator may also find the above items at random and seize the opportunity to commit fraud. In contrast to low technology offenders, high technology offenders are more efficient schemers and planners. They use

advanced methods to obtain information and plant an employee at a bank or a human resources centre to use them to obtain victims' information. They also create false websites that target vulnerable and gullible individuals who may be attracted to such websites and 'opportunities' to make 'quick profits'. They thus unwisely submit their personal information. Many people have fallen victim to identity theft through fake websites that offered jobs to unemployed individuals. This is ironic as victims who are in need of jobs and therefore vulnerable then submit sensitive and comprising information to scammers, unaware of the fact that they are being subjected to identity theft.

- Converting Information: Once in possession of personal information, a credit card, or an identity document, identity thieves use a variety of ways to convert information into a consumable form (Vieraitis et al., 2015:2). Identity thieves may call credit agencies and report that they need a duplicate credit card and, being in possession of the victim's personal information, the agency may be convinced and hand them a new credit card. Hoofnagle (2007:5) refers to this practice as "account takeover". The fraudsters may create these cards themselves using the victim's information. They then sell these credit cards or use them to purchase products to sell to unaware and sometimes aware customers at a cheaper price. According to Vieraitis (2015:2), these customers then resell these products to the general public in their respective communities. Being in possession of a victim's personal information, offenders may gain access to information that credit card companies send to their clients, and they thus use this information to withdraw money from the victim's account (Vieraitis, 2015:2). McNally and Newman (2005:57) state that if such information is in the hands of offenders, they may submit fraudulent tax returns and collect these returns for themselves.

The above information indicates the depth and width of identity theft and illustrates that there is a large pool of people involved in such criminal activities − from those that obtain physical objects such as bags and purses, to individuals that acquire useful and personal data they were given by snatchers or thieves in hi-tech fraudulent ways. This information is then further converted into a consumable product, which may be delegated to another person or group of thieves to divulge. As mentioned earlier, those who purchase these consumables may be aware of the criminal activity that was committed in order to acquire the goods that were sold to them. Police officials must thus

consider all parties involved during their investigations and the prosecution of identity theft perpetrators. Detaining one individual may thus not be enough as this person could easily be replaced by another with 'business continuing as usual'.

2.3 Causes of Identity Theft

According to Hoar (2007:2), any activity in which identity information is shared or made available to others creates an opportunity for identity theft. Companies must be sure not to divulge client information carelessly as this offers perpetrators the opportunity to commit fraudulent activities. In most cases, identity theft occurs due to the irregular flow of information from officials, banking organisations, and social media applications. These parties often withhold information as they are bound to do so by law or by company regulations. This then leaves civilians open as prey to identity theft perpetrators as they are unaware of the dangers that they should look out for to determine whether they are being scammed. Abubakar, Zadeh, Janicke and Howley (date) state that the development of "...a regulating scheme has been a challenge [as] factors such as the lack of standardization of protection [and] the establishment of a trusted online identity is *[sic]* proving difficult [due to] the increasing number of online users as well as the nature of the internet, which is borderless". These factors are some of the contributing factors that lead to identity theft.

2.4 Impact and Consequences of Identity Theft

According to Monahan (2009:3):
"True damage and real victimization lies *[sic]* in the sense of personal violation, psychological trauma, possible medical care, family issues, and other ill effects, which of course include the time and expense involved in trying to restore one's financial identity."

Due to a paucity of research on identity theft in South Africa and the fact that information had to be obtained mostly from cases from abroad, it may be argued that many South African citizens may not understand the magnitude and depth of identity theft in this country. The traumatic impact of this criminal phenomenon leaves victims financially and psychologically destitute. The reasons for this lack of information go far deeper than already mentioned (they will be discussed later),

and it is therefore important to make the public aware of the impact and consequences of identity theft. For instance, public awareness may forewarn citizens not to sympathise and assist where they can, as this will prevent them from succumbing to ruthless criminals. The impact and consequences of identity theft are briefly discussed in the next sub-sections.

2.4.1 Financial impact

"There is widespread agreement that identity theft causes financial damage to consumers, creditors, retail establishments, and the economy as a whole" (Hoofnagle, 2007:3). Gilbert and Archer (2011:4) make an important note by stipulating that victims who report the theft of a credit card will generally not be held responsible for the fraudulent activities that occur thereafter. This begs the question whether the financial consequences victims suffer *before* they report being victimised should still be for their account. Golladay and Holtfreter (2017:6) state that financial and legal costs are amongst the most severe consequences of identity theft as it is the most expensive compared to other criminal offenses.

In a paper exploring the issue of digital forensics − cybercrime in particular − Irons and Ophoff (2016:3) state: "ID theft is one particular variant of cybercrime". These researchers further state that approximately R3 billion per annum is lost to ID theft in South Africa. This supports the researcher's intention to investigate the policing of the identity theft phenomenon and to explore the role played by SAPS officials in reducing this amount that is lost each year by the economy due to this crime. According to SABRIC, the largest card fraud transpires when credit and debit card fraud is committed in the absence of an actual physical card, which is known as 'card not present' (CNP) loss (Brown, 2017). In such cases a credit card number was used.

The researcher focused solely on ID theft and fraud in the Durban Central area in KZN, which was a form of crime that constituted a high percentage of commercial crimes in 2012. It was mentioned in section 1.3 that the rates decreased in the three years thereafter and again picked up in 2016. Crime statistics from the South African Police Services Annual Crime Report (2018/2019: 172), reveals rates of commercial crimes over the past ten years, indicating an increase of 14.4% in commercial crimes between the year 2018 and 2019. According to this report, commercial crime

has an extensive impact and leaves a dent in the South African economy, affecting businesses, inflation in goods and services, and puts the running of many companies at risk (SAPS Annual Crime Report, 2018/2019: 172). “As most victims of identity theft can confirm, this phenomenon can destroy one’s credit record and even lead to costly litigation that takes years to correct” (Abubakar, Zadeh, Janicke and Howley, 2016).

2.4.2 Victim well-being

Victims experience different feelings post identity theft victimisation that are both physical and emotional. According to a survey conducted by Khan, Rakham and Bangera (2018:4), 40% of the participants in their study who had been victims of identity theft experienced stress and frustration, 42% admitted to feelings of mistrust and denial, 85% felt livid and infuriated by finding themselves in that particular situation, while 42% of the victims experienced difficulty trusting others, especially on social media platforms. Physical pain and injuries that were experienced were headaches, sleeping problems, dietary changes, stomach ache, muscle as well as back pain, and high blood pressure (Golladay and Holtfreter, 2017:9).

In Criminology studies students learn how the justice system and correctional services deal with offenders and victims. Victims are obligated to enter a process known as ‘restitution’. Victims generally face many different issues post identity theft victimisation, and restitution is thus a programme that aims to assist victims by supporting them to come to terms with the manner in which they were victimised, be it financially, physically, or emotionally. Whites and Fisher (2008:5) support the claim that this restitution programme is effective by stating that, in some instances, victims are granted a corrective victim criminal record which is issued by the courts. According to this record the victim is exonerated of all criminal records committed by identity theft syndicates in their name. However, the researcher questions the efficacy of these initiatives, or any other programmes, that was designed within the justice system with the purpose of assisting victims with regards to the consequences they were left to face post victimisation. This is evident in the Truth and Reconciliation Act (TRC) which only includes ‘any violation of human rights through the killing, abduction, torture or severe ill-treatment of any person’ (Pradier, Rubin, and van der Merwe, 2018:9). The efficacy of the TRC is further argued by The researcher further bares

such doubts from the lack of assistance expressed by previous victims of identity theft and fraud of receiving little to no help at all in clearing their names and gaining their identities back.

Victim Assistance: In the context of the USA, it is argued that "...victimization focuses on dollar loss and dismisses the emotional trauma or time needed to restore records and identity" (Golladay and Holtfreter, 2017: 3). The emotional damage suffered by identity theft victims is considered to be significantly high in this country where it is likened to physical assault, particularly if the victimisation has been repetitive. It is important for victims to know the first steps to take when they have been victimised. For instance, the following should be addressed:

- Which department, financial institution, credit reporting company, or agency should first be notify when the theft has been discovered?
- What information regarding the procedures and processes involved in the identity theft is required, and who should be contacted should there be any queries?
- What information will the investigating officer or team need in order to solve the case?
- Inform victims of honest estimates of the chances a case may be resolved, how they may be compensated, and what chances there are of recovering the identity document or card.
- Victims should be given/request referrals and contact numbers of person(s) who can further assist them should the agency that was approach no longer be able to provide help regarding their case.

Kempen (2016:1) provides pivotal information that is important for victims to be aware of what to do when they were victims of identity theft. The researcher believes that this should be done without putting any strain or pressure on the victim. What may be considered an obvious first step for all citizens to make sure that contact details of the financial/credit agency are readily available for immediate contact, some may not be aware of this and should thus make note of. The victim should then alert the affected credit company or bank that they have been a victim of fraud. The complainant should also acquire as much information as possible on how to go about preventing any more damage (Kempen, 2016:1). The victim should then gather as much information as possible proving their last transactions and point out the transactions and debt created by the fraudster. According to Kempen (2016:2), it is important to report and close that account immediately. Thereafter, the victim may report the crime to the SAPS by completing an affidavit.

All other investigations and inquiries should be made after the matter has been reported to the SAPS in order to assist in the urgent apprehension of the perpetrator. The victim, with the assistance of the credit company, must ensure that the account/s have been closed, thus preventing the perpetrator from further damaging the victim's credit and or debt account (Kempen, 2016:2). It is critical that information from both entities is relayed to all parties involved in the matter.

If everything is done to the letter, victims should not be held accountable for any costs suffered after they reported the identity theft. One can argue then that this means that individuals who are unaware that they were victims of this crime for a long period of time will have to account for the costs incurred by identity theft syndicates. The issue is whether, if an individual was unknowingly plunged into fraudulent theft over an extended period, the SAPS will assist in this situation as large amounts may have been spent by the perpetrator. Victims should not be held accountable for such fraud and thus the SAPS, credit bureaus, and the criminal justice system should devise ways to assist and compensate victims adequately.

2.5 Investigating Identity Theft

This study was premised on the role that the SAPS should play in policing identity theft. Such investigations are an integral part of policing and thus the following section will examine how both preliminary and continued investigations of identity theft are conducted. Due to a lack thereof literature in the South African context, the researcher relied on information from the US.

2.5.1 Preliminary investigation

According to the Ministry of Justice (2015:5), the investigation of a criminal event involves the following steps:

- Establishing and recording a report of an offence: When an individual has been a victim of a criminal offence, he is obliged to report the matter to the police. The investigation authority is then charged with the task of recording the event as described by the victim.

- Should the report be recorded by an officer who is not an investigation officer, the report is to be handed over to the correct authority.

2.5.2 Continued investigation

- The investigating officer is then responsible for conducting an investigation, doing so on the basis of the complainant's report and after having analysed and seen reason to believe that a crime has been committed.
- The head investigator is tasked with making the decision whether or not to continue with an investigation. This decision may be made by the investigating officer and is not dependent on the head investigating officer's decision.
- During the investigation, should the victim decide that he does not want the suspect to be charged and punished according to the law, the criminal investigation is discontinued.
- In the event of a physical injury, and the complainant or victim is unaware that he fell victim to a crime, the investigation may be initiated even if the victim did not request that the suspect be charged or an investigation be opened.
- The public prosecutor may, if supported by the law, open a case and press charges in the interest of the public even if the victim decides not to continue with the investigation.

The Ministry of Justice (2015:9) states that a criminal investigation may be postponed in order to acquire clarity regarding the information gathered or if the investigation is also related to another offence. This decision may only be taken by the lead investigating officer or authority and only if postponing the criminal investigation does not place a threat on the complainant's life or endanger him in any manner.

The above points are fraught with inconsistencies in the investigation of identity theft, and it was thus hypothesised in this study that it was due to these inconsistencies that identity theft investigations were impeded, resulting in very few cases being prosecuted. Pivotal to any criminal phenomenon is clear legislation, the efficient operations by police departments, and clarification of jurisdiction which will ultimately result in viable data being reported so that cases may be prosecuted and criminals brought to book (Whites and Fisher, 2009:9). Guiding victims through

the procedure of a case by updating and informing them of any changes or steps is critical in ensuring that cases are seen through to the end. The relationship between law enforcement/the SAPS and credit reporting agencies to ensure the communication of vital information is important as this will assist in building a case for the victim and improving their chances of not being held responsible for any criminal records committed under their identity.

2.6 Law Enforcement: Police Response to Identity theft

According to a report by the Center for Victims Research (2019) one of the reasons victims do not report identity theft incidences could be due to victims' unawareness of where to report an identity theft crime (Irvin-Erikson and Ricks, 2019: 10). This is probably due to obscure lines of communication and information within law enforcement with regards to the reporting of this crime. It is thus of pivotal importance to clearly and precisely make known the form and order of reporting identity theft to law enforcement agencies and that this is communicated widely to the general public.

Although this information may be viewed as common sense by any informed citizen, it is important to understand that many are unaware of the details of where and how to report crimes other than injury and property theft. Once the citizenry has been properly informed, victims will be aware of the first step to take when and if they find themselves victims of identity theft. This will not only encourage victims to report identity theft, but will ensure a more efficient police response. White and Fisher (2008:8) concur, arguing that miscommunication regarding where victims may and should report identity theft is a serious problem. They stipulate that there is currently no consistency in the manner in which police departments operate.

2.6.1 Effective police response to identity theft

In the USA, laws were passed and regulated to ensure that victims would know how and where to report any criminal incident. According to the United States Department of Justice (2012:31), legislation requires that the police should record allegations of crime regardless of the area where the crime occurred. Jurisdiction is thus not an issue in this country. However, if such cases were

reported in an unclear and unregulated manner, they may be left unattended by the police departments in either jurisdiction area (White and Fisher, 2008:8). For instance, if an incident occurred in the South African context in Durban central involving a victim who resides in Umlazi whose belongings were found in a suburb in Montclair, this would involve three police stations who will then be responsible for the investigation and arrest. Such inconsistencies should thus be corrected by police departments to allow the proper and fair handling of victims' cases.

According to White and Fisher (2008:9), effective police response to identity theft is further worsened by the lack of communication and sharing of information between credit reporting agencies and investigating officers. This may negatively affect victims' cases as information may be withheld by the agency which could otherwise have been helpful in the investigation. Instead, such investigations are hindered and are often not successful. Although this is a problem law enforcement is faced with, there are currently no policies or procedures in place to guide this required cross-referencing and relaying of information from credit reporting to law enforcement agencies. A disturbing fact is that financial institutions and credit reporting agencies use cost benefit analysis when it comes to identity theft measures. Therefore, as the costs of implementing and investigating these cases out-weigh the benefits the institution will receive, very little is done. This then ultimately leaves victims to rely heavily on law enforcement to help resolve their cases and restore their identity credibility.

Moreover, financial institutions seem to be unwilling to divulge information of their records and data breaches to law enforcement authorities as they deem the reputation of their respective institutions more important than the stolen identity of a client (Cassim, 2015:8). Walls (2013:2) concords and states that this is concerning as it makes the work of police officers more difficult, as they then do not have a complete understanding of the criminal advancements and evolving methods of identity theft used by syndicates. One thus questions the expectation of law enforcement authorities to effectively respond to and protect individuals from the scourge of identity theft.

According to the steps to follow when one has been a victim of identity theft, the Southern African Fraud Prevention Service (SAFPS) states that victims are required to prove their innocence to the

company or institution that they are currently in debt with, which could be more than one (Cassim, 2015:10). The researcher found this disturbing as, apart from the financial and emotional consequences of identity theft, victims are now expected to do the work of the company security staff and police investigators by gathering evidence in order to prove their innocence. Bearing in mind that this is only the first part of the process when victims wish to clear their name, this process has to occur before the victim reports the crime to the SAPS. For effective police response, it is vital that the police are alerted as soon as possible. Expecting victims to conduct their own investigations prior to reporting the case of ID theft to the SAPS is thus irrational and counterproductive.

The expectation of effective police response requires victims, credit reporting agencies and financial institutions to work in a conjoining effort to assist in locating the identity theft perpetrators. The prolonged procedure of victims gathering their own evidence and proving their innocence to the affected credit company or bank will negatively affect the process and timeframe of investigating the case and apprehending the perpetrator. Thus, in the researcher's view, exploring new and effective ways of going about clearing one's name and regaining one's identity should be reassessed. Consideration of victims' state of mind upon discovering that they are in debt for purchasing goods that they never did should be a priority. Moreover, any delay in reporting the offence because the victim tried in vain to prove their innocence to the credit company will hinder and delay the police investigation, and thus much time will be wasted.

As the responsibility for crime investigations is vested in the hands of the law, the police are mandated to assign a task force to specifically deal with certain cases. However, in terms of identity theft this has proven to be a problem. Whites and Fisher (2008:9) stipulate that assigning a task force to a case of identity theft has advantages such as obtaining a large body of information, utilising available resources, and obtaining varied expertise. "This often results in stronger and more thorough investigations, seamless continuity for a case through the stages of the justice process, and avoidance of duplicative efforts" (Newman and McNally, 2005:51). But although the functioning of task forces has been successful in many instances, they seem to be limited when it comes to identity theft. Setting up an identity theft task force requires large amounts and many

resources due to the high number of cases, and there are currently simply not enough resources to assign a task force to each identity theft case (Whites and Fisher, 2008:9).

According to Walls (2013:8), identity theft crimes have often been unique and many cases have fallen outside the police operating paradigm. These crimes are less visible in nature and harder to detect compared to known criminal theft offenses where property or an object was stolen. Therefore, although obliged to act and assist when victims report an identity theft incident, there is little that the police can do to support these victims. It is mandatory for the police to constantly monitor various current and evolving crimes regardless of the police culture that they have become accustomed to. The nature of the world we live in is constantly changing and developing and technology and crime, particularly the methods utilised to carry out hi-tech offenses, are no exception. Therefore, it is contingent upon all organisations, departments, institutions and individuals to work together to fast-track the prevention and detection of identity theft and prosecute these perpetrators.

2.6.2 Prevention measures and strategies: From apprehension to prosecution

As important as it is to raise public awareness concerning any criminal phenomena, one needs to be careful not to impose a concept of self-policing amongst the public. According to Monahan (2009:5), when victims are interrogated and positioned to assume responsibility for technological risks in order to avoid becoming victims of identity theft, this places the responsibility of protection and policing on the victim's shoulders, whereas it is the police who are in actual fact tasked with the responsibility of policing and protecting the general public. When victims are interrogated and questioned as to why they did not take any security measures to safeguard their software data or personal information, these victims are ultimately accused of "aiding and abetting [criminals] and [it is they who are] blamed for being an easy target and guilty for participating in the crime" (Monahan, 2009:5).

The Federal Trade Commission should act on behalf of victims and initiate strategies to deter, detect and defend victims. However, this involvement may obscure the line of who is responsible for protecting the public from criminal activity. Public awareness and the precautions people take

and the duty of police officers to police and protect the general public may be conflicted. During investigative procedures, police officers need to be careful not to place the onus on victims to take the necessary steps to protect themselves from being victimised. Therefore, although there are steps that can be taken to prevent this criminal event, police officers should be aware that ID theft syndicates constantly advance their methods and therefore victim blaming and imposing policing on victims should be avoided. If this is sustained, it may also contribute to the ill effects suffered by victims post victimisation. Any information that is not of assistance in investigating and prosecuting a case of identity theft should not be divulged as it may have other unfavourable effects on victims of identity theft.

2.7 Risk Assessment Strategies

2.7.1 Information security risk assessment

"An information security risk assessment (IRSA) [strategy] produces risk estimates, where risk is the product of the probability of occurrence of an event and the associated consequences for the given organization" (Wangen, Hallstensen, and Snekkenes, 2017:1). Although this is a method that is commonly used by companies and organisations, any case of identity theft should revert to an IRSA process. This is important for taking the necessary measures and precautions to avoid risks, and further account for possible consequences that may arise from potential risks. Risk assessment strategies can be measured with the help of victims, financial institutions, as well as the SAPS.

Moreover, it is important to conduct threat assessments to measure any potential and extent of harm and threat. Financial institutions, but more especially victims, possess authentic information pertaining to the intent as well as the potential harm that identity theft may cause. With enough numbers it would allow financial institutions to generalise the occurrence and potential harm of this crime, thus they may better equip themselves to prevent it from occurring. Police departments that most victims of crime reach out to for help will have a clear understanding of what they are dealing with and how to go about pursuing perpetrators. Although each organisation may conduct

their own investigations, working together with all role-players will greatly assist the deterrence of identity theft as well as the detection of threats.

According to Wangen, Hallstensen and Snekkenes (2017:1), information security, which is briefly referred to as InfoSec, is regulated on the basis of ensuring confidentiality, integrity, and the availability of information. This process requires clarification of risks and the continuous review of systems in place to detect any potential risks. Payment systems that facilitate online websites to negotiate transactions for the exchange of goods or monetary value and to carry out payments are utilised based on the decision by buyers. However, part of the responsibility should be placed on the seller as a company or an organisation, as they are also subject to adhere to the Protection of Personal Information (POPI) Act that requires all organisations to comply with its provisions to safeguard personal identifiable information. Outweighing the costs and benefits of carrying out online transactions should be measured by the seller who should then also devise resources to prevent fraudulent activities.

Identifying theft risk becomes imminent when a security system is in place, yet individuals often find themselves locked out of their device or online profile. Identity theft syndicates may purposely instigate this as they are aware of the security precautions and regulations that the systems utilise in order to retrieve passwords. The security system inadvertently allows the ID perpetrator to pose as the owner of the device or profile through this procedure, thus gaining full access of the victims' device and/or profile. Although going through the system may not necessarily be easy, it is also not difficult, and thus hackers are able "to use social engineering to crack 2FA, which is vulnerable if the device is stolen. All that is required is to accept the validation code" (Capps, 2017:2).

Turner and Holt (2012:7) argue that being knowledgeable about computer operating systems is a protective factor against becoming a victim of ID theft. They stipulate that if individuals are acquainted with such skills and knowledge, they may be able to detect and identify malicious websites and/or tactics insinuated by ID perpetrators. Although this is possible and may contribute significantly to a decrease in the number of victims, it may only really assist the younger generation as the older generation may only be knowledgeable about the basics of conducting online transactions.

2.7.2 Techniques to curb ID theft

The Department of Home Affairs (DHA) initiated a new system known as the Home Affairs Identification System (HANIS) (Cassim, 2015:10). The HANIS system aimed to address identity theft that is committed through the theft of identity documents by replacing the currently facilitated paper system with a digital database. According to Farelo and Morris (2006:4) a smartcard-ID was developed in order to combat and ensure individual identification by utilising a fingerprint system. Furthermore, a partnership was then established between SABRIC and the Department of Home Affairs which sought to permit banks to inquire for correspondence of personal identifying information from HANIS (Cassim, 2015:10).

A system was also created to monitor and detect the distribution of what is known as Personal Identifiable Information (PII) using a privacy regulator (Swart, Irwin and Gobler, 2016:1). The only issue concerning this system is that interference with data or data breaches can only be reported if they are detected. The time frame for data breaches to be detected by the regulator is stipulated to be a month, which leaves plenty of time for personal information to be discovered, used, or distributed and or sold to others for fraudulent use. There are thus many disadvantages regarding a privacy regulator, such as that data breaches could be established by a third party. The question posed by Swart, Irwin and Gobler (2016:3) is: Is there is a possibility that this third party can create the breach using PII and only report the data breach after misuse of an individual's PII has been reported? An automated system would thus decrease the time data are left to be discovered and manipulated by anyone who gains access. It should also prevent perpetrators from making copies of the compromised or unguarded data (Swart, Irwin and Gobler, (2016:9).

According to Capps (2017:2) of NuData Security, security systems entailing the use of a username and password were created to prevent hackers and fraudsters from gaining access to important data. As new forms of preventing hackers from gaining access improved, so did hackers' scamming methods to retrieve personal information. Many people tend to use familiar as well as one and the same password for all online websites. Capps (2017:2) states that this has become very easy for hackers to figure out, particularly when and if users have honestly answered and completed the regulatory questions required on websites when creating online profiles. The way

in which security systems operate, contrary to what many may believe, is designed not to lock out hackers but rather to make it difficult for them to gain access.

Biometrics is popularly used in the current era. Anderson, Durbin and Salinger (2008:13) state that biometric information is based on the physical traits and/or characteristics of a person which include fingerprints, signature, and retinal scans. Biometrics are part of three authentication techniques. The second is known as 'token-based authentication' that verifies that people are who they say they are, or that they own a particular profile or object by producing a type of authentication that only the owner of a profile will have, such as a driver's license with their information, an identity document or card, and a pay slip. The third technique is known as 'knowledge-based authentication' which refers to information that only the user or client will have knowledge of, such as the name of their favourite pet or a mother's maiden name. Cassim (2015:8, 9) states that, although there are means that make it highly difficult but not impossible for personal information to remain protected such as biometric authentication, this type of authentication is not affordable for all organisations and institutions.

Austin (2005:2) lists a few strategies and techniques that individuals may utilise in order to protect themselves from becoming victims:

- Victims should not engage in any unsolicited emails.
- Storing information on a computer system should be safeguarded by creating an encryption code in order to protect the stored data.
- Installation of security software, such as a firewall, and antivirus and anti-spyware is important. These systems and applications should be updated at regular intervals.
- Before disposing of a storage medium (USB), one must ensure that the files previously saved have been deleted and wiped and can no longer be restored should the USB be discovered by another individual.

Various businesses now provide such IT security services in South Africa, particularly to assist in protecting consumers and combating identity theft. Although these efforts are commendable, the figures surrounding this epidemic are still far too high for South Africans to be at ease. This calls for our law enforcement agencies to be more vigilant, to communicate their findings and strategies

to the general public, and of course withholding any information that could assist ID theft syndicates to improve their methods. All role-players should thus work together with communities to reduce and hopefully prevent the identity theft phenomenon. Sadly, it is a constant race between hackers/identity theft syndicates and security systems as technological advances evolve constantly. To prevent perpetrators from finding loopholes to gain access to people's personal information, security systems should always be one step ahead.

2.8 Policies that Address Identity Theft Internationally

According to Irons and Ophoff (2016:5), it is imperative to establish legislation that focuses on a particular criminal offense in order to govern, monitor and police specific crimes. This will allow efficient control as well as the prosecution of criminals who find themselves on the wrong side of that law. However, this seems to be a problem in the context of identity theft in South Africa as there is currently no legislation that governs this crime specifically. Instead, when victims report this crime, offenders may be prosecuted under the common law offense of theft, and not particularly identity theft. This may blur the lines as the term 'theft' is defined as the theft of property or physical objects and not personal information. The work of a criminologist is to assess and measure the effects of the law in deterring crime (Romanosky, Telang and Acquisti, 2011:7). Below is the examination of identity theft laws and policies from an International and National context.

2.8.1 United States of America

"Identity theft, which is perceived as one of the greatest threats to people's critical data, now represents the largest category of fraud-related complaints in the United States" (Monahan, 2009:1). According to the United States Government Accounting Office (2002:1), personal information includes an individual's name, social security number, address, date of birth, alien registration number, government passport number, driver's license, mother's maiden name, and biometric information such as fingerprints, a voice print, or a retina image.

Table 2.1: Types of identity theft that evolved in the USA

Era	Type of Identity Theft
1800-1918	The outlaws of this era killed people to assume their identities.
1919-1921	Identities were stolen to cast votes multiple times.
1922-1930	Smugglers created their own version of witness protection programs and murdered people to attain legal documents to create new identities.
1931-1959	Youngsters created fake IDs to buy alcohol.
1960-1969	Introduction of credit cards gave criminals new ways of identity theft.
1970-1989	Frank Abagnale, the infamous con artist, stole identities to cash cheques.
1990-1998	Technology advancement increased cases of identity crimes.
1999-2000	Introduction of Internet and search engines like Google led people to give away personal information.
2001-2003	Credit reporting agencies were instructed to provide credit reports on customers to prevent fraudulent accounts being opened.
2004-2015	The National Crime Victimization Survey was updated to include new forms of identity theft.
2016	Identity theft was the most popular consumer complaint for 15 consecutive years.
2017	American banks increased their security systems, causing criminals to use other platforms for stealing identities.
2018-2020	Technology was evolving and new apps were being introduced so that thieves were gaining more ready access to personal information through these new apps.

Source: (Irshad and Soomro, 2018:2).

Identity theft legislation to protect the rights of individuals was enacted and has now been in existence for many years. This is known as the Identity Theft and Assumption Deterrence Act of

1998 (Saunders and Zucker, 2010:1). According to Allison, Shuck and Lersch (2005:2), an offender may be punished by law if he "knowingly transfers or uses without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law". Offenders of identity theft are compelled to pay a maximum fine of $250 000 and may be detained for a maximum of 15 years (Saunders and Bucker, 2010:1).

An identity theft task force, which was established in 2006 by former President George Bush, made recommendations that looked at "keeping consumer data out of the hands of criminals, making it harder for criminals to exploit consumer data, making it easier for victims to detect and recover from identity theft, as well as increasing and prosecution of perpetrators" (Mathews, 2013:6). This resulted in the enactment of the Identity Theft Enforcement and Restitution Act of 2008. The researcher commends this Act for its consideration of the victim as it also focuses on the restitution of victims who suffered harm from identity theft. Although identity theft may be deemed a recently promulgated law in US legislation, all fifty states in the USA have recognised identity theft as a criminal offence since 2013 (Holtfreter et al., 2015:5).

Section 1 of the Computer Misuse Act of 1990 was enacted in order to address cybercrime. It is defined as a crime to obtain data without authorisation through the use of a computer (Manap et al., 2015:6). This Act was implemented in order to assist in addressing identity theft techniques such using spyware, Trojan Horse, and hacking, and to prosecute perpetrators under the above Act. Although identity theft is included in the Computer Misuse Act of 1990 under section 1, perpetrators who entice victims into sharing their personal information are not prosecuted under the Act due to the perception that victims voluntarily shared their personal information (Manap et al., 2015:6).

According to Martina (2017:40), privacy protection laws vary among the different states. The USA government enacted the Privacy Act of 1974, 5 U.S.C. 552a. According to Stevens (2003:12), this Act was established in order to protect citizens' personal information such as information "maintained by federal executive agencies, and to control the collection, use, and sharing of information" (Stevens, 2003:12). The Privacy Act governs the activities of both agencies and

organisations. However, according to Rotenberg (2001:1), people's rights based on the Privacy Act were quickly diminished after the September 11 attacks, also known as 9/11, which were terrorist attacks at a scale that had never before been seen in America. In efforts to prevent such devastating attacks from ever occurring again, new technological advances were devised. Surveillance was maximised by the state, meaning that all information − telephone records, banking records, voicemail records, etc. − can now be accessed by the state.

A lot of key perspectives of the privacy laws were weakened due to the enactment of the Patriot Act, which granted the Foreign Intelligence Surveillance Act to operate at a larger scale by expanding its operational territory (Rotenberg, 2001: 5). This Act further opened a pathway for police officers to conduct searches of citizens without a formal notification. Now this may ultimately allow certain individuals access to manipulate the system and commit extensive acts of identity theft and fraud due to the open access the Patriot Act permits the state.

Each decision made concerning the privacy, safety and security of the country and its citizens, should be done so with risks and threat opportunities in mind. Any action taken to protect could well enough result in destructive and worsened consequences.

2.8.2 India

Kumaraguru and Cranor (2014:1) explored perceptions of privacy in India and the USA and postulate that India faced various troubles that led to the enactment of the India Information Technology Act of 2000, which allows the monitoring of the misuse of technology and digital systems. Citizens of both India and the USA found themselves victims of identity theft. In one incident India was accused of outsourcing personal information when victims discovered that they had purchased appliances such as televisions in another state or province (Grant, 2006:3). This was attributed to an organisation known as the Business Process Outsourcing Industry in India that extended its service provision to companies in other countries, thus giving access to information of clientele from countries they provided their services to.

As the above Act lacked precision and thus rendered certain Acts non-criminal and not punishable by law, the Information Technology Amendment Act of 2008 was introduced into law (Varma and Khan, 2017:1). The IT Amended Act of 2008 outlaws the use of sensitive personal data, the introduction of viruses, the manipulation of accounts, denial of services, the use of phishing and spams, stolen computer resources, the unauthorised and misuse of communication devices and digital signatures, cheating, cyber terrorism, and child pornography. According to Varma and Khan (2017:4), section 43(h) of the IT Act as amended in 2008 protects the rights of individuals who are account holders of an Internet service provider (ISP). Section 66 C of the IT Amendment Act of 2008 addresses identity theft offenses and makes them punishable by law. These offenses include the fraudulent use of an electronic signature, a password, or any other unique identification feature of any person. This is punishable with imprisonment for a term of three years and a steep fine.

2.8.3 The United Kingdom (UK)

As identity theft crimes escalated in the UK (Cassim, 2015:23), measures had to be adopted to curb them. According to Meulen (2006:20), financial institutions and private corporations were the only organisations that were protected by law in terms of ID theft. Therefore, the Data Protection Act of 1998 (DPA) was passed and enacted by Parliament which allowed UK citizens the right to privacy and protection in terms of electronic records of personal information (Black, 2001:30). According to Holtfreter et al., (2015:5), financial losses associated with identity theft are estimated at 1.7 billion pounds each year in the UK. Rather than declining, these losses seem to increase each year. The enactment of the DPA initiated the operation of a new office under the Information Commissioner. This office governs and controls all aspects of information security and ensured the proper implementation of this law. Black (2001:32) states: “The Act authorizes the Commissioner to maintain a list of organizations that collect and use personal data, disseminate information about the Data Protection Act, promote and assist compliance with the Data Protection Principles, process complaints, and prosecute violations”. This differs from the USA and South Africa, where the law requires citizens to individually file or press charges against data breaches and the invasion of their privacy. In the UK, it is the Information Commissioner who deals with any violations pertaining to ID security.

Research has shown that the UK currently has no legislation that directly deals with or prohibits identity theft. According to Romanosky, Telang and Acquisti (2011:2), the Science and Technology Committee in the UK postulates that the enactment of a law against data breaches and disclosure will ensure the personal security of internet users. In its efforts to curb identity theft and fraud, the UK also initiated a forum known as the Identity Fraud Forum (IFF) as well as the Fraud Steering Committee (IFSC). These two bodies are mandated to implement measures to decrease the occurrence of identity theft and fraud. They are tasked to:

- identify new opportunities for data sharing across the public and private sectors;
- reduce fraud involving the impersonation of deceased persons;
- establish the cost of identity fraud to the UK economy on an ongoing basis; and
- research the impact of identity fraud on victims statistically and track those cases.

According to Martina (2017:38), an announcement was made by the European Commission regarding the reform of privacy legislation. The purpose of this proposal was "strengthening the protection of personal data as a fundamental right and creating new opportunities for the digital market". As was previously mentioned, there are no laws in the UK to protect citizens from identity theft or to outlaw it. Therefore, revisions of and strengthening of rights that protect citizens' rights in this regard are crucial to prevent harm to individuals. It has been over a decade since the approval of the Data Protection Directive in 1995 that aimed to effect pivotal changes in the IT sector. Another necessity for reform is that people who have direct access to the Internet have increased by large numbers, and this has resulted in more individuals potentially having open access to data. Social networks with large numbers of subscribers have emerged, thus ways of protecting the content and information resulting from these social interactions have to be considered. Martina (2017:38) states that the EU saw the necessity to relook at persons' privacy at an international level due to discussions that looked at sharing of information with other countries.

The above propositions resulted in the following:

- Regulation (EU) 2016/679, which replaces Directive N. 947/46/CE on data protection which applied directly in all EU member states[1] by 25 May 2018;

[1] The UK has since left the EU.

- The appointment of a Data Protection Officer under the auspices of the above Regulation;
- The introduction of Directive (EU) 2016/680 on the use of data by authorities with the aim of improving the prevention, investigation and criminalisation of crimes or executing penal sanctions, which replaces Decision 2008/977/GAI of the Council, and was supposed to be incorporated into national law by May 2018 (Martina, 2017:38).

Contrary to the absence of legislation that specifically speaks to and protects UK citizens from identity theft, the above stipulations are considered to have equipped the EU with "the most protective regional framework in the field of data protection" (Martina, 2017:38).

2.9 Policies that Address Identity Theft in South Africa

Ncube (2017:8) defines the common law of fraud as the "unlawful and intentional misrepresentation that causes actual prejudice or is potentially prejudicial to another". According to Cassim (2015:10), identity theft is embodied in common law, meaning that person(s) guilty of identity theft may be prosecuted for fraud, forgery, or altering a forged document, each of which is dependent on the specific case. Sentences for the above offenses range from a minimum of 15 years to as long as 25 years, with sentences imposed as per the Criminal Law Amendment Act No. 105 of 1997.

2.9.1 Protection of Personal Information Act No. 4 of 2013 (the POPI Act)

The Protection of Personal Information Act No. 4 of 2013 (the so-called POPI Act) is a legislation that was established to protect the personal identifiable information of the public. Krishnamurthy and Wills (2009) refer to personal identifiable information as any information that enables another person access one's personal identity. According to Botha, Swart and Eloff (2015:5), this piece of legislation is a privacy law in favour of protecting every individual and organisation in terms of how their personal information is handled. The POPI Act was enacted to reduce the commission of identity theft (Cassim, 2015:11). Moreover, it was introduced due to the increasing practice of identity theft, invasion of privacy, and data breaches which included hacking the personal information of victims (Swart, Irwin and Grobler, 2016:2). According to Cassim (2015:11), the

POPI Act seeks to reinforce section 14 of the Constitution of the Republic of South Africa (Act No. 108 of 1996), which stipulates that everyone has the right to privacy. POPI includes, apart from the right to privacy, the right to protection against the unlawful collection, retention, dissemination and use of personal information.

The POPI Act requires all organisations to adopt and be in compliance with this Act, and if any organisation or person is found guilty of contravening this Act it may result in "damage to a company's reputation, loss of customers, [inability] to attract new customers, pay-outs in damages as a result of civil class action, fines of up to R10 million, as well facing jail time of up to 10 years" (Botha, Swart and Eloff, 2015:4). The consequences for non-compliance with the POPI Act have serious implications for organisations that disseminate customer information without the consent of customers and clients. Research further states that organisations that have not yet adopted this Act and utilise other strategies are advised to use these strategies along with the POPI Act principles. This Act is and will be of great assistance in protecting civilian information from being accessed by identity theft syndicates. According to Swart, Irwin and Grobler (2016:3), the POPI Act comprises of eight principles:

- Accountability, section 8
- Processing limitation, section 9 to 12
- Purpose specification, section 13 and 14
- Further processing limitation, section 15
- Information quality, section, 16
- Openness, sections 17 and 18
- Security safeguards, section 19 to 22
- Data subject participation, section 23 to 25

2.9.2 Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

The Electronic Communications and Transactions Act No. 25 of 2002 (ECT) has been in existence and utilised for more than 10 years in South Africa (Eiselen, 2014:2). This Act encompasses ecommerce, privacy issues, electronic government services, domain names, as well as cybercrime.

Prior to the promulgation of the POPI Act, the ECT Act was utilised to protect personal information and to present cases of data breaches and identity theft in court (Swart, Irwin, and Gobler, 2016:6). According to Farelo and Morris (2006:5), Chapter 3 of the ECT Act addressed the use of cyber inspectors while Chapter 4 is based on the governance of cybercrimes and fighting network crimes. When this Act was promulgated, there had been no mandate that addressed the commission of crimes such as identity theft and child pornography and international corporations could not effectively fight to eradicate IT viruses and other known criminal cybercrimes. It seems that the more reformed we strive to be as a country, the more we attract opportunities for criminal activities. The ECT Act was thus implemented to guide and protect government as well as all citizens and prevent malicious acts co-ordinated through the use of advanced technology.

2.10 Conclusion

The above discourse regarding identity theft in various countries and under various conditions revealed that losses due to identity theft-related crimes are unacceptably high. This is to say that, as troubled as South Africa is regarding identity theft and its policing, this criminal phenomenon is a worldwide scourge that affects many individuals all over the globe. The countries that were referred to might seem better equipped than South Africa to battle identity theft, but recent technology advancements have placed all countries at high risk. The situation regarding identity theft was discussed in the context of South Africa as well as first world and developing countries, and issues pertaining to the detection and prevention of identity theft were highlighted. It was clear that many aspects of this form of crime require urgent consideration as the methods facilitated in developed countries such as the USA may not necessarily be generalised to South Africa. In general, though, resources that are dedicated towards combating and preventing identity theft-related technological advancements should be reassessed and revitalised. The theoretical framework that formed the basic premise of understanding identity theft and its causes will be discussed in the next chapter.

CHAPTER THREE
THEORETICAL FRAMEWORK

3.1 Introduction

As is evident in many studies, social phenomena are explained by employing certain theories that illuminate their occurrence. In the current study three theories, namely the rational choice theory, the routine activities theory, and the human identification theory, were used to explain the criminological phenomena (identity theft and fraud) under study. The rational choice theory (RCT) is used to explain why perpetrators commit identity theft, while the routine activities theory (RAT) explains how identity theft occurs. The human identification theory (HIT) explains how and why individuals fall victim to identity theft.

According to Burke (2017:8), theories are not necessarily observed literally, but researchers use them to support or refute the findings that emerge from the data they collected. For the purpose of this research, the selected theories will be used to explain and extend the knowledge that was garnered regarding the identity theft and fraud phenomena. Further research may support the theories that explain what is understood about identity theft and what is already known about identity theft.

3.2 The Rational Choice Theory (RCT)

3.2.1 Origin of the rational choice theory

According to Cornish and Clarke (2013:22), RCT came about from a general shift in focus that occurred in the 1970s within British Criminology. Most of its foundation is owed to Cesare Beccaria, who is known as the Father of Criminology. The main tenets of RCT are explained by Cornish and Clarke (1983), who are extensively cited in the following discourse. The basis of this theory was formulated as it introduced a critical shift from the radical behaviourist perspective, which postulates that "criminal behaviour is primarily the result of long standing criminal

predispositions and psychopathologies that cause individuals to offend" (Cornish and Clarke, 2016:22). When it became evident that offending behaviour was primarily influenced by an individual's environment and situation, this led to a shift in perspective, which led radical behaviourists to explore the decision making of offenders. This shift introduced the choice model that at first focused on the gambling phenomenon which had originally been viewed by economists and decision theorists as an irrational choice, but which then began to appear to be more rational than had been assumed earlier (Cornish and Clarke, 2016:23). Criminological literature provides a description of "the convergence of interest among a variety of academic disciplines, [the] sociology of deviance, criminology, economics, and cognitive psychology upon a conception of crime as the outcome of rational choices on the part of offenders" (Cornish and Clarke, 2016:24). The above points out the fundamental basis of the RCT is embedded in the understanding that an individual's choice to commit a crime is rational and not irrational.

3.2.2 Rational choice theory components

To outline the basis of this theory, RCT argues that criminal behavior is rational as opposed to irrational. The main tenets of this theory postulate that criminal activity is premeditated, meaning that it is thought through and carefully planned before it is committed. The actions of criminals do not occur by chance or by mistake; rather, crimes are purposively acted out. RCT is thus defined as "when people make choices based on cost-benefit analysis" (Haycraft, 2013:20). RCT comprises of six components and four decision-making models:

3.2.2.1 Criminal behaviour is purposive

People are guided by certain beliefs, needs and desires to act or conduct according to certain behaviour (Cornish and Clarke, 2016:32). Cornish and Clarke (2016:32) stipulate that these beliefs and needs, together with actions, give meaning to behavior and make it purposive for the individual. RCT thus adopts the standpoint that "...crimes are purposive and deliberate acts that are committed with the intention of benefiting the offender" (Cornish and Clarke, 2016:32). In the case of identity thieves, many of their actions are purposive in nature because, whatever the intention of theft may be, the outcome/s will benefit the offender (Cornish and Clarke, 2016:32).

These outcomes may be sexual gratification, revenge, or the acquisition of materialistic items or goods, but it is mostly the acquisition of money that is of most benefit and what identity thieves seek to gain, as money enables the thief to purchase or acquire the aforementioned benefits.

3.2.2.2 Criminal behaviour is rational

RCT asserts that peoples' actions are not only purposive in nature, but also rational. Individuals will lay out their goal and assess the best possible way to attain it (Cornish and Clarke, 2016:33). According to Cornish and Clarke (2016:33), actual criminal behaviours differ according to conditions and situations as some may entail less than perfect circumstances and time pressures. Another uncertainty in criminal behaviour is that risks accompany criminal activity while the influence of drugs and alcohol also plays a role in determining the outcome of the behavior that is dependent on the offender's experience − yet experience does not guarantee a perfect outcome (Cornish and Clarke, 2016:33). These authors further argue that identity thieves are seen as rational beings as many of their actions are calculated and thorough. This is evident in the evolving nature of and advancements in defrauding that have extended to cybercrime and various ways in which identity perpetrators have developed their methods of identity theft (Cornish and Clarke, 2016:33). RCT emphasises that some of these actions take place under less than perfect circumstances, which explains why the sloppiness of ID perpetrators often ultimately leads to their apprehension. "Criminal decision-making is by its very nature prone to error because of the constraints under which it has to operate" (Cornish and Clarke, 2013:26).

3.2.2.3 Criminal decision-making is crime specific

RCT makes reference to a third concept that emphasises that many make the mistake of viewing crime as one unitary phenomenon. This led to the development of theories and policies that seek to explain the commission of crime according to the nature of particular crimes (Cornish and Clarke, 2016:34). According to Cornish and Clarke (2016:34), this concept encourages the examination of crime according to the particular crimes that perpetrators seek to commit. "Offenders don't commit crime, but carry out specific crimes, each of which has its own particular motives, purposes, and benefits" (Cornish and Clarke, 2016:34). Crimes differ and so do people's

decision to commit them as they first weigh the benefits of committing the offence of choice. In identity theft, for instance, the reasons for committing this crime differ. The Southern Association of Forensic Scientists (2012) stipulates that identity theft may be facilitated in order to commit financial fraud which includes, but is not limited to, bank fraud, credit card fraud, computer and telecommunications fraud, social program fraud, tax refund fraud, as well as mail refund fraud. Identity theft can also be used to carry out criminal activities such as computer- and cybercrime, drug trafficking, organised crime, alien smuggling, and money laundering (Cornish and Clarke, 2016:34).

3.2.2.4 Distinguishing criminal involvement from event decision

According to the RCT, there are one of two ways in which an offender or potential offender may be involved in a criminal offense, namely through criminal involvement decisions and criminal event decisions (Cornish and Clarke, 1985). Criminal involvement decisions is a phrase that refers to conspiring and assisting in the planning of the actual crime. It is concerned with an individual's criminal career and includes decisions about initial involvement (initiation), continued involvement (habituation), and desistance (ceasing action or stopping) (Cornish and Clarke, 1985). These theorists stipulate that involvement decisions differ according to the crime and should thus be studied differently for each crime. The decisions regarding continuation (habituation) and desistance may also differ according to the crime. Lastly, Cornish and Clarke (2016:36) argue that crimes such as identity theft are, according to the RCT, seen as economically vital. This is in contrast to the crime of paedophilia where decisions concerning continuation and desistance are based on sexual gratification and not on financial gain.

RCT not only explains identity theft, but it further assists in unpacking this phenomenon. Whilst the first two concepts seek to explain identity theft as being executed purposively and rationally by the perpetrator, the last two concepts are viewed by the researcher as a means of psychologically understanding the criminal involvement and decision making of the perpetrator. The theory thus emphasises the importance of treating and investigating various crimes in a non-unitary manner by considering that criminal decisions differ for each crime and should thus be examined in a manner that implies so.

3.3 The Routine Activity Theory (RAT)

3.3.1 Origin of RAT

The routine activity theory, commonly known as RAT, was developed by Cohen and Felson (1979). RAT is a sociological theory that is based on the premise that criminal events are the direct result of the presence of a likely offender and a suitable target, and the absence of a capable guardian. The premise of RAT stipulates that "the aggregate changes in legitimate opportunity structures, coupled with the lack of capable guardianship, will increase the convergence in time and space of motivated offender and suitable target (Pratt, Holtfreter and Reisig, 2010:3). The three characteristics of RAT will be discussed next.

3.3.2 Characteristics of the routine activity theory

3.3.2.1 Absence of a capable guardian

According to Chamard (2007:1), RAT endorses the notion that a crime is committed in the presence of an offender coming into contact with a suitable target in the absence of a capable offender. This premise is applicable to identity theft perpetrators but with a notable extension. The absence of a capable guardian can refer to the absence of persons in close proximity to an item or a person (a suitable target). In the context of the current study, the researcher understands the absence of a capable guardian as the lack of security, be it formal or informal, that prompts the commission of the crime of identity theft. It is important to note that the theory was initially exclusive of cybercrime. The researcher's stance of capable guardianship in relation to identity theft thus defines a capable guardian as any security measure that is in place to prevent identity theft by perpetrators. This means security measures that prevent them from stealing another person's identity online as well as formal and informal policing measures that prevent this crime from being committed. The absence of these 'capable guardians' thus allows potential identity theft perpetrators to see their opportunity and to commit this crime. Miro (2014:1) states that one of the implications of RAT is that the presence of a capable guardian should not be understood as the assurance that a crime will not be committed. This is different for identity theft as security

measures and systems – such as biometrics − may hinder the occurrence of a crime as these data are hard to copy or steal in order to gain access to an individual's personal information (Clark, 1984).

3.3.2.2 Suitable target

A suitable target is defined as a person, object or property that may be threatened by an offender, with emphasis on the term target as opposed to victim as, in most cases, perpetrators target valuables, goods, or property and not necessarily a person in the absence of a guardian (or security) (Sherman, Gartin and Buerger, 1989). With regards to identity theft, a suitable target may be multiple online users who utilise computers to assist them with functions such as online shopping, banking, and many other activities that are habitually conducted online such as social media where personal information can be required and accessed upon registration to a social account (Kempen, 2016:1). Identity theft entails a broad spectrum of criminal activities and is inclusive of grant recipients who may also be vulnerable to perpetrators. On their way to collect their grant money, they may be suitable targets, especially in the absence of an individual who accompanies them. Cohen and Felson (1979) highlight four attributes or characteristics that enhance the suitability of a target, namely value, inertia, visibility, and access (VIVA):

- Value: Something of value and that which may be useful according to the offender.
- Inertia: The size, weight and shape of the physical aspects of the person or item that act as an obstacle/impediment to the offender seeing it as a suitable target.
- Visibility: An object's visibility, or the exposure of targets to offenders, or the attribute that marks the person or item for attack. For example, a grant recipient who walks alone and carries the SASSA card, or posting pictures of one's valuables or possessions on social media or online.
- Access: Access refers to the location of the possession or item that increases accessibility and the risk of an attack as it is within reach of the likely offender.

3.3.2.3 Likely offender

According to Pratt, Holfreter and Reisig (2010:2), fraud perpetrators are increasingly using the Internet to attract suitable targets. This can be done when a likely offender poses as a service provider under a false identity in order to gain access to a suitable target's information. In Cohen and Felson's (1979) initial theory, emphasis was placed on direct contact of the likely offender with the suitable target. However, advancements in the methods utilised by ID theft syndicates have enabled likely offenders to commit a crime without being in close proximity to the suitable target as they use the Internet and thus avoid "direct contact [when] taking or damaging [the] property or possessions of the suitable target" (Glaser, 1971:4). Based on the premise that the likely offender and a suitable target have to be present in the same space and at the same time, individuals may still find themselves suitable targets for ID theft perpetrators who take their personal belongings (such as ID documents, credit cards, account numbers, and passwords) and use them for fraudulent activities. Grant recipients who may follow a consistent routine when collecting their grant money on a specific day and use the same route to reach their destination may be easy targets for likely offenders who may grab the opportunity to defraud them in the absence of a suitable guardian.

The researcher has stipulated how identity perpetrators have surpassed the common pattern and premises of RAT, of committing crime in the presence and direct contact of the likely offender and suitable target, property or object. The absence of capable guardianship which with id theft both the initial premise of actual persons (formal and informal police) being present applies as well as capable guardian also referring to security systems preventing id theft syndicates from accessing personal information of online users for fraud. Identity theft can thus be linked to and explained by the routine activities theory by adding and explaining the advanced methods that the theory does not account for.

3.4 The Human Identification Theory

3.4.1 Introduction

The human identification theory was developed by Professor Roger Clarke in 1994 when he wrote a paper titled *Human identification in information systems* for the *Information Technology and People Journal*. The researcher borrowed this theory from the Information Technology discipline as it links with the criminological phenomena under study. Human identification was Professor Clarke's way of identifying and portraying the vulnerability of civilians to identity theft.

3.4.2 Characteristics of the human identification theory

This theory explains how and why individuals become victims of identity theft and fraud. Initially, the human identification theory sought to explain the likelihood of individuals becoming victims of identity theft and identity fraud. Professor Clark (1994) proposes three characteristics that enable a person(s) to use any other person's details under false pretence (Lo Plucki, 2001:8).

Kodl and Lokay (2001:2) define human identification as the association of data with a particular human being. In practice, an individual can be granted access or recognition if, and should, they be authenticated. Generally, this means that the requesting individual should be able to provide information confirming that they are who they claim (Kodl and Lokay, 2001:2). This may involve a variety of techniques that are known as 'token based authentication', 'knowledge based authentication', and biometrics (Anderson, Durbin and Salinger, 2008:13). These are explained as follows:

- Token based authentication is when an object (a physical item) that only the user possesses is used to authenticate him/her, for example a driver's license or an identity document.
- Knowledge based authentication is when a person is recognised or identified by showing that s/he is in possession of information that only s/he will know. This information is for example a social security number or a mothers' maiden name.
- Biometrics are physical characteristic such as a signature, a DNA pattern, a description of appearance, a retinal scan, or fingerprints.

The theory is linked to the topic under discussion it was developed in an attempt to prevent identity theft. Professor Clarke assumed the positon of identity theft victims and proposed the aforementioned characteristics in the effort to combat identity theft. Some of the characteristics that the theory refers to have long been in place as many security processes require the possession of an identity document or finger prints and social security number. Lo Plucki (2008:9) states that the above security measures may easily be known to perpetrators without the victim being aware, which underscores why many individuals fall victim to identity theft and fraud. Information that is supposedly meant to be private and known by only a specific individual or organisation are easily stolen by identity theft syndicates while the victim only discovers the fact when it is too late. Kodl and Lokay (2001:1) published a paper with the intention of extending the existing theory of human identification. In this paper they list various means of formal identification. Their work focuses on the authentication used by organisations for transactions made by employees (Kodl and Lokay, 2001:3). Publications after this theory was developed serve only as an improvement and an extension of Professor Clarke's work on human identification.

3.5 Summary

Identity theft was explained with reference to three sociological theories. It was explained that RCT informs the reasoning and logic behind committing identity theft by various criminals and that this theory emphasises the importance of treating crime in a non-unitary manner. The researcher argued that RAT explains how identity theft occurs according to the significance of time and place and the presence and/or absence of cable guardianship. With regards to identity theft, RAT was discussed and it was explained how this theory relates to both the physical theft of identity documents as well as the online theft of individuals' identity details. The researcher also referred to the human identification theory that professor Clarke developed to explain how various forms of authentication are used to differentiate among people and to prove identification by linking personal data to an individual. Various measures have been taken by organisations and companies to improve the authentication systems of personnel and clients in order to protect them and prevent identity theft. The following chapter will present an in-depth discussion on the methodology and techniques that were utilised to collect the data.

CHAPTER FOUR
RESEARCH DESIGN AND METHODOLOGY

4.1 Introduction

A researcher who understands the direction that the chosen research project should take will select a specific manner of research and suitable methods to employ to bring it to fruition. When this is done, the researcher will have a framework and concept of inquiry which s/he may constantly review for guidance in terms of the approach to each aspect of the research (Wahyuni, 2012:5). In this chapter, the methodology that the researcher employed will be discussed in line with the purpose and objectives of the study.

This chapter includes a geographical description of where the study was conducted. Although Durban Central is mentioned as the study location, the target population was the Serious Commercial Crime Unit of the SAPS from which the sample was drawn. The Durban Central Business District is a complex urban setting and occupies a wide geographical area. Thus, for the purpose of the study, only a relevant target population within the larger city population was selected.

This chapter includes information regarding the research design, the methodological approach, the sample selection procedure and size, as well as the data analysis approach. The type of data analysis for this qualitative study may be deemed somewhat questionable as it has rarely been used, and therefore the NVIVO software that facilitated and assisted the analysis process that was used is explained and validated in detail. Pivotal to conducting research is the need to adhere to ethical procedures that will ensure the validity and trustworthiness of a study. For instance, all parties involved need to be comfortable and given assurance of the confidentiality of their participation and views. All these measures will be thoroughly discussed in this chapter.

4.2 Significance of an Investigative Study

The type of study a researcher selects depends on the goal and or aim of the research (Asenahabi, Busula and Ronoh, 2019:1). The rationale of a study mostly stems from observations and the discoveries made by the researcher upon the review of related literature. In this process a nexus is found that assists the researcher to unfold the niche of the research. The escalation on the crime of identity theft, as well as the evolving nature of identity theft operations, prompted the researcher to explore the policing of this crime. As this was an investigative study, the researcher was allowed not simply to explore the topic, but to question deeper into the strategies and functions of the SAPS unit under study. This enabled the researcher to extract underlying and earlier unnoticed data pertaining to the phenomena under study.

4.3 Research Paradigm

It is imperative when selecting a research design that the researcher assumes a paradigm in which the study will function and that will give direction to the study. Wahyuni (2012:2) defines a research paradigm as a way of thinking and a manner in which a researcher perceives the world. Much emphasis on the importance of establishing a research paradigm as it guides and assists the researcher from wandering into their own beliefs and perspective (Rahi, 2017:1). For the purpose of this study, the interpretive paradigm was adopted. According to Wahyuni (2012:4), interpretivism is structured around what it is known as constructivism. These research inquirers believe that reality is socially constructed, which means that reality exists in how individuals perceive things and what their actions are when they encounter these things (Gemma, 2018:9).

Due to the belief that human experiences and actions are subjective, there is a constant shift and multiple perceptions of what social reality is (Wahyuni, 2012:4). Although a research paradigm may go unnoticed in the work of a researcher, it plays a huge role in practice as it affects and controls how a researcher approaches and answers certain questions (Rahi, 2017:1). The methodological approach that was selected was the qualitative approach. This allowed the researcher to conduct interviews with recruited participants in order to obtain their different opinions and perceptions as they experienced identity theft from the perspective of their

involvement in the SAPS unit under investigation. This approach is part and parcel of the interpretivist way of thinking in research (Wahyuni, 2012:4).

A relatively new perspective within the qualitative approach has emerged which argues that, unlike other forms of inquiry, no research inquiry is more accurate than the other. Rather, it is pivotal for researchers to assess the appropriateness of a research practice to effectively unpack the phenomenon being studied (Gergen, Josselson and Freeman, 2015:2). It was thus important for the researcher to understand the goal and objectives of the research and the value that it will have before choosing the research approach. The research questions were also important as they would guide the approach that would best answer the questions. After having taken all the above into consideration, the research approach and design were determined (Wayhuni, 2012:5).

4.4 Research Design

For the purpose of this study, the researcher utilised the phenomenological approach to research. According to Creswell (2007:74), phenomenology is a methodological approach that is mostly used to understand social life. Crime is a social phenomenon, and phenomenology was thus the most appropriate approach to study and understand identity theft. The reason for this is that this type of inquiry seeks to understand the perspective of knowledgeable participants concerning the topic being studied (Creswell, 2007:34). This approach allows the researcher to listen to and examine the taken-for-granted perspectives on a social phenomenon with the use of interview questions. This type of inquiry also allows individuals to expose their lived experiences and share their expressions of those experiences to provide context, insight and substance to the findings of a study (Johnson and Parry, 2016:49). The way of thinking that shapes a study is aligned with the researcher's particular interests and values regarding a topic. The phenomenological perspective is a way of thinking that owes its historical foundations to sociology and philosophy (Taylor, Bodgan and DeVault, 2015:4).

4.5 Study Location

The data were collected at the John Ross House Offices of the Serious Commercial Crime Unit of the SAPS. This building is located at 21-26 Margarate Mncadi Avenue, Johnson Lane, Durban. The interviews were conducted in secure venues on the 10th Floor of this office block. John Ross is described as a historic building which was named after a historic adventurer.

4.6 Research Methodology

"A research methodology is a philosophically situated plan of inquiry, orienting the choice of particular data collection and data analysis methods and linking them to the desired aims of research" (Johnson and Parry, 2016:48). The foregoing thus implies that the type of research methodology a researcher chooses maps out a plan of the necessary steps that the researcher will follow when conducting the research.

4.6.1 Research approach

When conceptualising a study and contemplating the research proposal or plan, the research design is a fundamental component that guides the manner in which the research will be conducted. Methodology generally drives the methods that the research inquirer will follow in the execution of the study. It is this method that will determine how the research questions will be approached and answered (Taylor, Bogdan and DeVault, 2015:3). The chosen approach for this study was the qualitative research approach.

The researcher chose this particular approach as it allows flexibility and recursiveness. The qualitative approach was chosen above the quantitative approach which is a rather fixed and linear approach to research and thus requires a pre-planned guide that the researcher is obliged to use to conduct the research according to a pre-planned design, which limits recursiveness. According to Maxwell (2012:2), "plans are made when entering or going to field sites, but upon arrival the whole plan may be changed, as "facts on the ground change our best laid plans". The qualitative approach

thus treats research as a real-life entity and thus renders the investigation subject to real-life events and consequences (Maxwell, 2012:3).

According to Mayan (2016:11), research inquirers may utilise a qualitative approach with the desire to understand the meaning and in-depth details that emerge from numbers and statistics associated with a phenomenon. This was this researcher's reasoning for utilising a qualitative inquiry, as she wanted to understand the story behind the continuing rise in identity theft incidences. It was also paramount to understand the gap between the structures involved in preventing and dealing with the identity theft scourge, and to explore the actual issues faced by these structures in their efforts to combat this criminal offence. There was no better approach than the one selected to extract the desired information and to make sense of the data.

4.6.2 Qualitative data collection

4.6.2.1 Data collection sources and procedures

"To understand the social world from the experiences and subjective meanings that people attach to it, interpretivist researchers favour to interact and have a dialogue with the studied participants" (Wahyuni, 2012:4). In this study, the researcher used both primary and secondary data. Primary data were collected by means of semi-structured individual interviews using open-ended questions as the aim was to investigate and gain insight into the phenomena of identity theft and fraud from the perspectives of the participants.

Secondary data were obtained by reviewing and scrutinising various scholarly articles, books, and journals. Scholarly search engines were also used such as Google Scholar, Ebsco Host, and Sabinet. The data that were collected from these secondary sources ensured the use of academically sound and reliable sources of information. As a student of the University of KwaZulu-Natal (UKZN), the researcher made use of the Malherbe Library at Howard Campus as well as other academic facilities offered on the Westville Campus.

4.6.2.2 Interview questions

Face-to-face interviews were conducted with 12 participants. Neuman (2014:347) stipulates that "face-to-face interviews have the highest response rates and permit the longest and most complex questions". The researcher utilised contingency open-ended questions when interviewing the SAPS SCCU officials in KZN Province. The questions that were posed applied to policing procedures during investigations to uncover and curb identity theft (Neuman, 2014: 331). The interviews allowed the researcher to gain in-depth understanding of the participants' views of identity theft. Rosenthal (2016:2) stipulates that when conducting in-depth interviews, it is important to pose open-ended questions that allow a free-flow of ideas and information as well as probing, as these elicit deeper understanding of the underlying factors and influences associated with the phenomena under study. The researcher was thus able to extract information on identity theft issues and concerns from purposively selected SAPS officials who were experienced investigators of this crime.

4.6.3 Sampling

According to Neuman (2014:246), the majority of empirical studies use sampling, but the type of sampling method depends on the specific study. The purpose of sampling in qualitative research is that the population is usually too large to involve in its entirely in the study, and thus relevant categories of respondents need to be identified within the target population (Neuman, 2014:247). For this purpose, two sampling methods were used, namely purposive sampling followed by snowball sampling. According to Sharma (2017:4) purposive sampling are participants selected by the researcher based on their usefulness to the study. Snowball sampling is characterised by referral of an initially selected few participants whom fit the research criteria (Parker, Scott and Geddes, 2019:4). These participants are then requested to refer the researcher to other knowledgeable participants. Purposive sampling was done to collect data from initially identified knowledgeable research participants, while snowball sampling had to be used to recruit additional participants with the assistance of the initial research participants. By utilising these two methods, the researcher elicited information from participants who possessed authentic knowledge regarding the matter under investigation.

The SAPS SCCU is a unit that was established to deal with all known (and uncover unknown) commercial crimes. The researcher approached the SAPS offices at the John Ross House and requested to speak to the Unit Commander. An appointment to see the Commander was set, and upon the researchers' return the purpose of the study was detailed to the Commander and their assistance in identifying other relevant participants. The latter were requested to refer potential participants who would be most likely to have information regarding the policing of identity theft. By using snowball sampling, the Unit Commander whom was purposively selected, assisted the researcher to recruit members within the SCCU who were likely to have information regarding identity theft. Although the SAPS SCUU consists of 40-60 police officials, the researcher sampled a total of 12 SAPS SCCU officials. Ten of these participants were police detectives while two were higher ranking officers in this unit with managerial experience. The length of the interview process varied for each participant, the least being 20 minutes and the longest_ one hour and 54 minutes (1h54minutes). All interviews were conducted during working hours, in each participants' work space (office). Only one out of the 12 interviews was conducted in the board room, where staff meetings are held.

The researcher specifically chose police detectives as they deal with commercial crime investigations on a daily basis. It was thus envisaged that these officers would be likely to have the most authentic information that the researcher was interested in. The two sampling methods that were employed were suitable as they ensured that the collection of ambiguous information and irrelevant data was avoided. Although researchers strive for generalisability of the data and the emergent findings, the use of in-depth interviews intends to extract deep understanding and meaning about behaviour and the social phenomenon under study in a limited location and study area (Rosenthal, 2016:3). The relatively small sample size and the demarcation of the study area thus means that the data may not be generalised to all SAPS units involved in identity theft investigations.

4.6.4 Methods of data analysis

According to Green, Willis, Small, Hughes, Smalls, Welch, Daly (2007:1), data analysis must occur concurrently with data collection. Instead of the familiar process of qualitative content analysis, the researcher accessed thematic analysis guided by a qualitative data analysis software.

4.6.4.1 Data analysis

To ensure that data analysis occurred concurrently with data collection, the researcher utilised the thematic analysis approach. Braun and Clark (2006:74) define thematic analysis as "...a method of identifying, analysing and reporting patterns". It is important to understand at the outset that the use of the software that will be discussed later was a keyword search facility after the data had been transcribed and processed according to the key steps as described below.

Although the interviews were conducted in English as all the participants were proficient in this language, it is important to state that some participants responded interchangeably in IsiZulu and English, others in isiXhosa and English. The data was then translated and noted as per interview verbatim. During the interviews the data were voice-recorded with the permission of the participants while field (observational) notes were also made surreptitiously so as not to disturb the flow of the participants' narratives. After each interview, the data were listened to very carefully and transcribed into a Word document by the researcher. The responses were transcribed under each participant's name and code for later uploading into the software search programme.

Once the narratives had been collected and transcribed (12 interviews were conducted in total), the researcher immersed herself in the transcription process and familiarised herself with the data by reading and re-reading the narratives. Thematic analysis was then conducted. This is a process that involves the coding of qualitative information and data. Therefore, the researcher engaged in a process of identifying relevant themes as they emerged from the data by means of key words and phrases. This process was assisted with the use of the software programme that will be described later.

In the process of thematic analysis, the researcher sought to identify specific patterns within the data as contained in the narrative content (Yardley, 2004:57). According to Clarke and Braun (2013:4), thematic analysis should not be viewed as a linear model, but rather as a process whereby the researcher may return to the previous phase should changes be required or errors be found. This is known as the 'recursive phase'. Thematic analysis comprises six steps or phases. As verbal interviews were conducted, thematic analysis was the appropriate approach to extract the data (Joffe, 2012:6).

The first step was to become familiar with the data. This step applies to all forms of qualitative analysis processes. Clarke and Braun (2013:4) state that it is important for the researcher to become immersed in the data. Thus the researcher repetitively read the interview transcriptions and focused on "noticing any observations" (Clarke and Braun, 2013:4). This step was carried out on the NVIVO software where all recordings were stored, transcribed and imported onto the software.

The second step of thematic analysis is that of coding. This process emphasises the importance of the above step of familiarisation, as the researcher will then be able to extract data that are relevant for the purpose of the research. In this process, the data were organised and categorised under headings, for example 'policing and the nature of identity theft in KZN Province'. This ensured focus and a guideline that avoided dwelling on irrelevant data. These codes and coding frames were extracted as the process was guided by the research objectives (Yardley, 2004:59). Coding and categorising of data was made possible and more efficient through the use of nodes and trees utilised on the software that will be further elaborated later.

The third step was to 'search for themes' (Clarke and Braun, 2013:4). The already coded data were again coded, which means that similarities within the data were identified and the themes that emerged were organised according to the research questions.

The fourth step of this process was to review the themes. In this process the researcher cross examined the themes against the coded data in order to ensure that the themes well represented the data that they were derived from. To ensure that the data were well represented in the themes that had been formulated, it was important to analyse and examine each theme. This process enabled

the researcher to give a detailed description of the meaning of the data in each theme. This process was somewhat less rigorous as the software had already identified similar words and patterns, which were colour coded by the researcher and categorised under the respective theme. Simultaneously, the researcher had to see how each theme fitted into the data and was pivotal to the study. After this had been done, the researcher determined if each theme was aptly identified or if new names for the themes needed to be constructed (Clarke and Braun, 2013:5).

The final process was to 'write up' the findings based on the coded key words and themes the software 'search facility' had produced. According to Clarke and Braun (2013:5), this technique is a crucial aspect in thematic analysis and involves weaving the data together in text. This process entails ensuring that the themes and content are consistent with the premise of the study, and linking the data to pre-existing literature that is related to the study and or that collected by the researcher.

4.6.4.2 Using the NVIVO software

The researcher made use of the NVIVO technique to assist in organising the data. NVIVO is a type of 'search' software that identifies patterns and similar ideas in the data (Bazeley and Jackson, 2015:1). According to Bazeley and Jackson (2013:1), this software was created to support data analysis in complex and advanced qualitative studies. This particular technique is known to be a powerful software tool that sifts through and organises extensive amounts of data (Bazeley and Jackson, 2013:1). Many make the mistake of assuming that this software analyses the data for the researcher to ensure less work, but this is not the case as this software only makes processes such as flexibility, trustworthiness, and transparency more reliable (Kaefer, Roper and Sinha, 2015:1).

Bazeley and Jackson (2013:2) state a few advantages of utilising the NVIVO technique:

- **Manage Data:** NVIVO is useful in keeping record of not only interviews and questionnaires, but recorded audios, images, videos, diagrams, and web pages (Bazeley and Jackson 2013:2). Using the software was extremely useful as all my data, particularly the recorded interviews were all stored safely and accessed whenever necessary.

- **Manage Idea:** According to Bazeley and Jackson (2013:2), this software may be used during data analysis as, in this process, the researcher can store any form of data and ideas (conceptual and theoretical knowledge) for later access. Using this function helped the researcher avoid the loss of important notes and ideas, by accessing the information at a later stage.
- **Query data:** This technique is relevant as, during research, the researcher may come across extensive and complex data, which may prompt the researcher to ask questions or query the data collected before (Bazeley and Jackson, 2013:2). This process thus helps the researcher to ask or query, and the relevant information will be provided and made available by the software.
- **Visualise data:** This process assists the researcher by showing (visually) aspects such as sampling strategies, content at each point of the researcher's interpretive and or analysis stage, and also relationships amongst ideas and concepts within the data (Bazeley and Jackson, 2013:2). Identifying a relationship and similarity amongst concepts was of pivotal importance to the researcher due to the qualitative stance assumed by the study. Thus identification of likeness in ideas allowed the researcher to generalise certain aspects of the findings crucial to the study.
- **Report from the data:** This can be achieved by "using contents of the qualitative database, including information about and in the original data sources, the ideas and knowledge developed from them, and the process by which these outcomes were reached" (Bazeley and Jackson, 2013:2).

4.6.4.3 Steps in using the NVIVO software

Hilal and Alabri (2013:3) list the following steps that need to be followed when using the NVIVO software.

- Working with Qualitative Data Files: In this step the researcher is advised to conduct all interviews digitally or electronically, which was done in this study. The electronically recorded interviews are to be saved according to each interviewee's name. The researcher is then required to transcribe the interviews into a word processing document and save the transcribed document onto the software. The saved file is imported onto the software by

selecting the document the researcher intends to import. According to Hilal and Alabri (2013:4), the software can automatically import the selected files onto the application.

- Working with ‘nodes’: This is known as a place within the software where references are stored. This location can later be accessed and used to code text or data. Hilal and Alabri (2013:4) state that there are two types of nodes, namely ‘tree’ and ‘free’. Each node stores all the information concerning a specific category or concept.
- Coding qualitative data: When coding text from a project document under a node or tree, the researcher or user is required to highlight the text in which they wish to code and drag it to the designated node (Hilal and Alabri. 2013:4). Once this is done, the highlighted text automatically changes colour. The now coded text then appeared on the right hand side where the coded stripe is located on the software. The researcher was able to allocate or code the same text with multiple nodes. The researcher then went on to analyse the text. Coding using the software, is a step found and used in thematic analysis, the difference being, the researcher used the NVIVO software to help code the data, faster and efficiently. The researcher thereafter, went on to analyse the coded and categorised data as required in thematic analysis.

NVIVO software is known for its fast and efficient data management, thus it is able to handle and manage different bulks of information at the same time, which has proven difficult manually or through qualitative content analysis. It lessens the complexity of data. When data are complex or broad and ambiguous, it is difficult and strenuous to sift through the volumes of data and analyse the content. Therefore, the software’s ability to reduce complexity is a huge advantage. “Moreover, the software’s searching and modelling tools allow making data visible in ways not possible with manual methods, allowing for new insights and reflections on a project” (Kaefer, Roper and Sinha, 2015:1). This signifies the eligibility and efficiency of this software, which has become a preferred method of qualitative data analysis.

Improvement in methodological rigor, consistency, and transparency are known features of this software, which were difficult to achieve before in qualitative content analysis. By facilitating the NVIVO software for the study, the researcher was able to achieve the aforementioned ethical and methodological consistencies. Hilal and Alabri (2013:5) state that not only is the software efficient,

but it has resulted in qualitative studies that have yielded prominent and professional results. With the assistance of the NVIVO software, the researcher was able to upload participant responses and identify the most commonly mentioned and similar ideas discussed by them. The NVIVO software organised the data efficiently and allowed the researcher to achieve ethical and methodological precision.

4.6.5 Methods to ensure Trustworthiness

The qualitative approach has often been viewed as inferior to the quantitative approach, which is of course not the case as the former approach is the most appropriate for studying human behaviour and perceptions. However, it remains important to ensure trustworthiness when this approach is facilitated. In the current study, the NVIVO software assured analytical flexibility, which did not limit the researcher to a single manner of analysis but rather allowed the inquirer to use that which best suited the study. It further ensured "enhanced transparency and trustworthiness of a qualitative study" (Kaefer, Roper and Sinha, 2015:1).

4.6.5.1 Reliability

Haradhan (2017:2) defines reliability as the degree to which the findings are true as well as ones' faith in the data collected. Reliability was ensured through the manner in which the interview process was structured. Furthermore, the concise yet precise data managing software utilised in the study known as the NVIVO software, ensured a flexible analytical process and the inclusion of data only relevant to the topic of interest.

4.6.5.2 Credibility

According to Cope (2014:1), credibility refers to the extent of truth in participants' views and the data collected from them. The question "*How congruent are the findings with reality?*" (Shenton, 2004:2) is thus important. This was achieved by applying the six steps of data analysis (such as familiarising oneself with the data to determine if they addressed the topic under study). The credibility of a study is determined by the familiarity and ease with which others are able to

recognise the experiences shared by participants. Moreover, Morse (2015:1) postulates that prolonged engagement with a study ensures credibility. The researchers' use of face-to-face, open-ended interviews with the research participants allowed participant observation and confirmation of the data. Through this manner of acquiring information, the researcher achieved prolonged engagement with the participants, and probing for and extracting new information that would otherwise not have been gathered also addressed this requirement.

4.6.5.3 Confirmability

Confirmability, which is a requirement in qualitative research to account for objectivity, refers to the degree to which the results can be confirmed or corroborated by others (Trochim, 2007:1). By using the method of triangulation and seeking the insight of a person who was familiar with the phenomenon of identity theft (in this case the study supervisor), the researcher was able to ensure the objectivity and credibility of the data that were analysed. Cope (2014:2) stipulates that confirmability may also be achieved by demonstrating and explaining how the researcher arrived at a conclusion, which further points to the fact that the findings are a direct result of the data that were collected.

Confirmability, which implies objectivity in a study, was also achieved through the use of the NVIVO software, as the researcher could not alter the software to achieve subjective results in any way. Rather, the software was able to analyse the authentic data using objective tools and techniques to an extent that the researcher might not have been able to achieve. Thus, at no point were the data altered to yield results favoured by the researcher.

4.6.5.4 Dependability

Dependability refers to consistency in the findings when the study is replicated twice in conditions similar to the initial study. Credibility precedes dependability − thus in order to ensure dependability, credibility has to be strictly adhered to (Shenton, 2004:3). Cope (2014:2) concurs with this notion by stating that dependability is achieved by ensuring that another is present to support and confirm the data collected by the researcher. Morse (2015:2) stipulates that

overlapping and multiple methods need to be used in order to ensure that a study is dependable. Therefore, by using the NVIVO software that is known for its precision and for yielding professional results, the researcher's confidence in achieving dependability in this study is unwavering.

4.6.5.5 Transferability

Transferability is a qualitative alternative to external validity in quantitative research. It refers to "the degree and extent to which the findings of a study can be generalized and repeated in similar conditions" (Trochim, 2007:1). According to Cope (2014:4), the findings of a study meet the transferability criterion when individuals who are not involved in the study understand and associate the results with their own experiences. The researcher proposed to achieve the above by ensuring that all conditions of the study, including aspects such as time and place, were emphasised and stipulated and were indeed stated during the interviews.

Morse (2015:2) states that, to further ensure transferability, the researcher's use of thick description is incumbent. The researcher met this criterion through the use of open-ended questions that were posed during face-to-face interviews. This naturally allowed the researcher to acquire in-depth and thick descriptions of the information the participants volunteered concerning identity theft. The researcher believes that she phrased the questions well in order to entice appropriate and relevant information needed to address the research objectives of the study. In this manner the transferability of the study was ensured.

4.7 Ethical Considerations

According to Schwartz (2016:40), the aim of the SAPS Research Guidelines is to safeguard and protect the rights of research participants. These ethics protect participants' right to privacy, dignity and well-being (Schwartz, 2016:40). The SAPS National Instruction 1/2006 also states that the term 'researcher' refers to "...the person who applies for access to a record or information in the possession or under the control of the service for the purpose of conducting research" (SAPS,

2006:1). The researcher therefore applied for ethical clearance from the SAPS Research Ethics Committee to conduct the study.

"You have moral professional obligation to be ethical even when research participants are unaware of or unconcerned about ethics" (Neuman, 2014:145). In light of this statement, the researcher recruited the participants and explained the purpose and the nature of the study to them before the interviews commenced. The researcher was also aware of the risk of physical harm, psychological abuse, and legal jeopardy, and thus adhered to all ethical requirements to avoid any harm the participants might have been subjected to (Neuman, 2014:148).

All the necessary channels to recruit and involve the participants were followed rigorously. As per the Human and Social Sciences Research Ethics (HSSREC) guidelines, the researcher applied for permission from the UKZN Ethical Committee and SAPS CCU to conduct the study among SAPS members, and permission was granted (Appendix A: Letters of Approval). The researcher also adhered to section 1 of the guidelines to ensure the scientific validity of the study, particularly with regards to consistency in the aims and objectives and the critical questions. Section 3 makes note of gatekeeper permission, and such a letter was compiled and sent to the SAPS CCU. In it the researcher requesting permission to be granted access onto the premises. This did not include consent to conduct research.

4.7.1 Confidentiality and Anonymity

Consent was also requested from and granted by each individual participant in writing to take part in the study. The participants were assured of their confidentiality and privacy/anonymity and that the information they provided would be presented in such a way that it could not be traced to them as individuals. Section 4.2 notes the importance of participants' confirmation of consent and their right to withdraw from the study should there be any inappropriate or negative consequences, and the participants were assured of this as well. The signatures of the participants were also obtained to confirm their voluntary participation.

4.7.2 Beneficence

Conducting research should somehow be beneficial to the research participants and community (Dimitrios, Antigoni and Kotrotsiou, 2018: 3). The study thus allowed for the expression of any challenges encountered by participants in their line of work. The mere knowledge of their issues being considered, allows somewhat of a relief in terms of their needs being regarded and their psychological well-being catered to. Furthermore, the researcher explained to participants the importance of the study and it's benefit to the Police Department, community and scholarly community, which participants conceded and were thus more than willing to contribute to such growth and change.

4.7.3 Non-Maleficence

For willingness and ease to take part in a study it is important to guarantee participants of the safety of doing so. As required in ethical conduct, is first ensure the study will be of no harm to participants (Rubenfield and Artal, 2017:2). Questions provided to participants were first approved by the Head Office in Pretoria. Participants were assured of emotional, mental and physical safety prior to the interviewing session. A tad wary of the questions that were to be asked, the researcher reassured those participants that all questions were based on the work executed by the participants. The researcher further reiterated as noted on the consent form, the participants' right to terminate the interview at the experience of any discomfort concerning the questions embarked on.

4.8 Limitations of the study

Although the location of the study is in Durban's CBD. There is no direct transportation to the SCCU offices, which required the researcher to travel on foot to collect information and conduct the study. Secondly, as aforementioned in Chapter 5, the intense workload the staff members are burdened with is quite immense which although the participants were more than willing to assist there was not a convenient and consistent time in which the interviews were conducted. The Researcher was thus forced to interview whomever was available at the time. In many instances appointments were rescheduled due to pressing responsibilities and commitments that were vital

for them (participants) to attend. Lastly, research requires the indication of a great deal of literature, with a topic of interest such as ID Theft and Fraud, little information is still yet available particularly in the South African context. Therefore, the above limited the researcher in their expression of the intensity of the pandemic.

4.9 Conclusion

The chapter offered a descriptive analysis of the methods that were employed to address the aim, objectives, and research questions of the study. The discourse accentuated the premise that motivated the type of methodology adopted by the researcher. The data collection and analysis methods were discussed, and the appropriateness of the techniques that were utilised was highlighted. The various channels that were pivotal to and preceded the execution of this research study were clearly expounded. The chapter that follows will present and critically discuss the data that were collected in the study.

CHAPTER FIVE
DATA ANALYSIS AND EVALUATION

5.1 Introduction

In the time and space of human existence, technological advancements have eased the lives of people and enhanced development. Even in the current age of modernity, criminals use old and new methods to commit fraudulent acts (Button and Cross, 2017:1). In this chapter the researcher will present and analyse the views of police officials with regards to identity theft, with particular reference to the rational choice theory, the routine activity theory, and the human identification theory and their explanations of criminal behaviour. Furthermore, the researcher will draw on the findings of previous researchers for the purposes of comparison and confirmation. Each participant will be referred to by pseudonym (e.g., P1 for Participant Number 1). It is important to note that some participants responded in isiZulu, some in isiXhosa, and others in English. The researcher then translated and transcribed these responses into English. The participants' comments are presented verbatim and are unedited for authenticity.

Various themes emerged from the data that were elicited during the semi-structured interviews;

Nature of ID Theft and Fraud:

- Modus Operandi (MO) used in ID Theft and Fraud Incidents
- ID Theft and Fraud Prevalence
- ID Theft with the Intention of Opening False Accounts
- Fraudulent marriages
- Interception of Digital Money Transfers
- Identity theft to trade in counterfeit goods
- ID Theft and Fraud Victims
- Causes of ID Theft and Fraud

Preventative Measures for ID Theft and Fraud:

- Procedural mandate of the SCCU

- Response to the call to Curb ID Theft and Fraud by the SCCU
- Measures Taken upon Discovering ID theft and Fraud Incidents
- Usefulness of an Automated Identifying System
- Awareness Campaigns as a Preventative Measure

Challenges Experienced by the SCCU in Response to and Prevention of ID Theft and Fraud:

- Limited Manpower and Inadequate Resources,
- Noncompliance by Implicated Organisations and Departments

5.2 Nature of ID Theft and Fraud

5.2.1 The Modus Operandi used in ID Theft and Fraud Incidents

The participants were well able to describe the Modus Operandi (MO) of fraudsters and ID thieves. Modus operandi can be defined as "all of the behaviours that are prerequisite to a particular offender successfully perpetrating a crime" (Collie and Greene, 2019:2). In order to combat and develop protective measures against a phenomenon, it is paramount to know about and understand the methods used by perpetrators to commit a particular crime. It is also noteworthy that the participants had investigated different cases, were working in different offices, and had varying levels of education and experiences, but they agreed on the MO of perpetrators when they engaged in specific crimes. For instance, various cases were mentioned as each floor within the SCCU works on differing cases (the 12th floor for example deals with cases associated with corruption). Each floor will be assigned a different type of fraud or identity theft case to investigate, and the investigating officers there becomes quite adept at dealing with each type of case. P2 argued that working within the Unit required a certain level of education and experience and that graduates were prepared for the pressure and insight required to work within the commercial crime field in order to understand the MO of perpetrators. The participants offered the following insights:

P1: *"Fraudulent marriages [are] prevalent mostly amongst foreign nationals, Pakistanis. They steal identity documents usually belonging to Indian women. They do so as to lower or eliminate any form of suspicion due to the [same] colour of their skin. Whereas marriage between a Pakistani and a Black African woman would be suspicious and result in maybe further*

investigation by the marriage officiator such as the Department of Home Affairs. Victims of identity theft in connection to fraudulent marriages were many in Phoenix. The reason for this is a large number of the Indian community is found in Phoenix."

P2: *"The stealing and use of another person's qualification for employment purpose. Foreign nationals, who commit fraud for the purpose of accessing a social grant or pension fund. They do this by stealing an identity document belonging to another person and use it to access the above."*

Below are more examples of their experiences and insights:

P2: *"Another common form of fraud that we as a Unit receive cases on is, the intercepting of money transfers. For example, you're selling a house, and you're expecting to receive an amount of R1 million into your account. The perpetrator then intercepts an email that the buyer is about to receive and changes the account details of the individual who is supposed to receive the transferred money. The buyer will then receive the account number as listed by the perpetrator, with the money then going into the perpetrator's account. The email does not look suspicious as it entails the bank's details and stamp of approval. The buyer will receive this email as if it were from the selling individual's bank. ... Or they may intercept the email from the seller to the buyer, change the account details and forward the email to the buyer. The seller may call to check with the buyer if they received the email sent by them. The buyer will then confirm to the perpetrator who is pretending to be the seller having received the email without any suspicion."*

P3: *"Most common form is that committed by employees, where you find that employees collude. This usually occurs during voids or when stores have discounts, then employees see this as an opportunity to steal from their employer...Pyramid schemes, which involve perpetrators creating a misrepresentation of a money generating platform. Perpetrators convince victims to invest their money in the scheme in exchange for double or triple the amount after a certain number of days or months."*

P4: *"Identity document theft, where you find a victim has lost their ID. Perpetrators use the victim's details which include their ID number, name, surname and date of birth."*

P5: *"Stealing of ID's and opening accounts. Some even go to the extent of buying houses and cars using your ID."*

P6: *"Opening of false accounts, such as bank accounts to commit fraud. They submit false company documentation. Opening of accounts in other peoples' names in order to misuse the account. Stealing another person's identity in order to seize their intellectual property or their Facebook accounts. There's a lot of Internet fraud currently occurring. Hacking of people's emails and impersonating the owner of the email in order to commit fraud."*

P7: *"Stealing of IDs to open accounts and loans or to make insurance claims from organisations such as the Road Accident Fund, which is currently are quiet common."*

P8: *"When a person loses their ID and you get a letter of demand that you owe a certain amount of money for a contract. Perpetrators normally steal IDs to get into cell phone contracts. The reason that perpetrators prefer taking cell phone contracts is because they can be done over the phone with call centres. This is easier and very successful for the perpetrators as they are able to give the consultant a stolen or false identity without the consultant knowing as they are not physically in front of them. The contract is entered into with the perpetrator confirming the details of the contract over the phone. Perpetrators may take as many as 5 to 10 phones, very expensive phones. The main purpose for such is to sell these cell phones. The victim of the stolen identity is only aware of such when he or she receives letters of demands or phone calls about money that they owe.... It could also be vehicles. Enter into a deal of purchasing a car through a consultant. Perpetrator gets a vehicle finance authorised through a consultant from call centre. The perpetrator then, with the reference number authorised by the consultant, goes to any car dealership and provides them with the authorisation from a banking institute consultant. The dealership then checks the details of the authorisation by phoning the bank, which confirms as they do have the details and ID number that were provided to them by the perpetrator. The dealership then sells the car to the perpetrator who then takes the car across the border. By the time claims of the contract are received by the victim, whose details were provided by the perpetrator as his own, the perpetrator is long gone."*

P9: *"Stealing of IDs and opening fraudulent accounts*."

P10: *"Mostly identity document and account takeover. Impersonating another individual and taking over their account."*

An important trend is the one distinguished by P1, who stipulated that Pakistanis were most likely to be perpetrators of fraudulent marriages using Indian women as victims. This revealed a viable

and pivotal characteristic that can be used during investigations of this type of fraudulent act. This trend can also be noted when dealing with fraudulent marriages amongst other ethnic groups. Although marriage between different races is not completely out of the norm, it is scrutinised in contrast to marriage between persons of the same ethnic group. In light of this fact, one may infer that it is contingent on authorities not to make marriages difficult or tormenting, but to confirm that they are all true in nature and intent. Furthermore, they need to ensure that an individual is who they claim to be, more so amongst those of similar ethnicity. This again highlights the importance of identifying and keeping record of the MO that occur repetitively for various crimes.

A common method that was mentioned by the participants (P1, P4, P5, and P7) is the theft of identity documents. This suggests that obtaining others' IDs is a prime cause of identity theft in order to commit fraud. Although IDs were said to be used for various types of fraudulent activities by each investigating officer, it is important to note that they echoed the same sentiment, namely that the theft of ID documents is a prevalent crime. Thus, based on the latter, one can deduce that the theft of IDs ultimately leads to a type of identity theft and fraud.

The detailed and extensive amount of information provided by the participants can be associated with each participant's experience and involvement in cases of identity theft in the Commercial Crime Unit. The depth in relaying the manner in which these crimes are conducted is noteworthy as this is evidence that each investigating officer's involvement in the cases that were investigated was authentic and that their understandings were not merely based on hearsay. The detailed responses by P2 and P8 are a case in point, as these participants, as well as the others, shared this information to the best of their knowledge.

The responses revealed that the most predominant methods utilised by ID perpetrators and syndicates are highly technological in nature. The modus operandi that they use as was referred to by P2 seem to be parallel with the tactics of high technology offenders, as was referred to in Chapter Two. The extent of planning and the depth of the methods involved in executing their plans, such as the interception of emails as stated by P2, indicate extensive syndicate operations that will target any person. This finding thus corroborates the statement that was made in Chapter

Two that it is essential to understand and counteract the MO of ID thieves if this crime is to be eradicated.

5.2.2 ID Theft and Fraud Prevalence

The participants unanimously viewed identity theft as rife in their area of responsibility. However, although this phenomenon was escalating with many such cases being reported and investigated, there were minimal cases of identity theft that they as the Serious Commercial Crime Unit could investigate due to monetary value stipulations. This means that this unit is mandated to investigate theft and fraudulent cases above a certain monetary value. Below are some of the responses indicating which cases were forwarded to the SCCU. For the purpose of this study, the participants were able to comment on the prevalence and severity of cases due to their many years of experience in the SCCU. This was evident in the response of P2 who had worked in the Unit for most of his career. The following was said by P2 when asked about the nature and extent of identity theft and fraud:

P2: *"That is dependent on each Unit, but yes, there are a lot of cases of identity theft. Although there aren't as many cases that we receive. Reason being as a Unit we have a certain scope that we deal with. If a case is under R100 000 we do not work on that case. SCCU is a specialising unit, therefore we only take cases that meet our threshold of R100 0000 and over. For example, if a perpetrator has used someone's identity to commit fraud of an amount lower than R100 000, such a case remains and is solved by police stations."*

This comment was supported by P3, who argued that there were relatively many cases of identity theft. Although she dealt with cases of fraud, she was not oblivious to the existence of cases of identity theft that were forwarded to the Unit for further investigation:

P3: *"Yes, although we only deal with fraud related cases. For example, people who create a misrepresentation of a platform that generates money. Our mandate states that we only take cases of a value or figure exceeding R500 000. All other cases of fraud which have a value less than R500 000 are investigated and dealt with at police stations."*

P10: *"That's a different question to answer, because cases are first opened at police stations, then if they can't handle the case or it does not fall under their mandate it goes to the Provincial Task*

Team Commission Crime and Provincial Office. The ones they do not attend to, then go to the Commercial Crime Unit. There is a procedure that is followed. I have a case that I am currently working on, but do not hear from other detectives if they also have [it] and are working on identity theft cases."

The above comments clarified the mandate of this particular Unit, stipulating that not all cases concerning identity theft and fraud are opened and investigated by the SCCU. Rather, cases are referred for further investigation from local police stations when and if they do not have enough resources to investigate the case and the monetary value incurred by the crime is to the value of R100 000 and above.

The participants concurred that the SCCU only investigates cases that meet the minimum threshold of R100 000. Only when local police stations fail to solve cases of identity theft and fraud below R100 000 will they be referred to this Unit. Based on the above, measuring the exact extent of this Unit's, and by extension the SAPS's, ability to curb and investigate identity theft was thus a tad difficult as not all cases of identity theft and fraud are reported to the SCCU for investigation. However, it was deduced that the severity of identity theft and fraud is rife, as the participants were able to attest to this due to their extensive experience in the force. The data thus supported the researcher's objective to examine the criminal phenomenon of identity theft and confirm its existence and widespread occurrence in the KZN Province. The participants were able to attest to this fact regardless of the minimal to average number of cases of ID theft that was referred to this Unit.

Unequivocally pivotal to curbing the crime of identity theft and fraud is the creation of awareness and eliciting information that will assist in curbing these phenomena. In this regard, the respondents commented as follows when they were asked when the crime of identity theft and fraud was likely to occur during the year:

P1: *"No, it is not seasonal. Identity theft can and occurs at any time of the year. Police stations will probably note that it is common around December, Christmas days when perpetrators will open accounts in stores. The SCCU receives dockets at any time brought to the unit by a police station."*

P2: *"No, identity theft and fraud is not seasonal, it occurs throughout the year, but it mostly spikes during the December holidays. Reason for this is due to a lot of movement happening, people coming from other provinces for example Johannesburg to visit and check into hotels here in Durban. Identity theft occurs in many ways. People who check into hotels use their credit cards, resulting in their information being left on a system that identity theft perpetrators set up. Others will check into restaurants, where you find that a waiter or a waitress has been bribed and works for identity theft syndicates. Customers will swipe their cards and enter their credit card pin which is copied and left on the system that the perpetrators has set up. Perpetrators will then create clones of the victim's cards and use them to withdraw money."*

P6: *"I would say that it occurs throughout the year. It does pick up during the Festive Season because that's when people are a lot more vulnerable. People are more likely to be out there spending a lot of money during such times, so identity theft syndicates take advantage of that. Even with banking systems where they are usually a lot stricter when it comes to certain purchases with the use of a credit card, you'll find that during the festive Christmas season, when a person purchases a product that they are not generally prone to buying, they wouldn't question such a purchase due to it being that time of the year when people normally buy or make large purchases. Identity theft syndicates then take advantage of such knowledge and use it to commit their crimes. They are then more on the prowl than they usually are during the year."*

P9: *"It occurs throughout the year, but it peaks during the Festive Season. You find that during the Festive Season even amateurs and disorganised criminals commit crime.*

P10: *"It occurs throughout the year and at any time, but when it comes to fraud it peaks mostly in December during the Festive Season. This is due to the fact that people disperse their Stokvel*[2] *money during this time, others receive work bonuses, and others are retiring or resigning. Those who have money spend it recklessly."*

According to the participants, identity theft is not a seasonal phenomenon but occurs throughout the year. Most also concurred that it peaked in December which is known as the Festive Season. This finding relates to what RAT proposes about the routine activities of people and also to what is clear in P6's response, namely that the Festive Season is generally known for large purchases. Spending more money has become routine for most citizens during the month of December, which

[2] A system according to which money is shared and banked that is popular in traditional African communities.

perpetrators have identified and now use as an opportunity for financial gain. In fact, the opening of accounts and large purchases by perpetrators is unlikely to raise questions. Furthermore, during this time of the year many spend money more recklessly and the majority of people are not guarded, which makes them easy and 'suitable' targets, as proposed by RAT. In view of the latter, one can deduce that, with the absence of guardianship (such as authenticity questions) by businesses such as car dealerships and stores, suitable targets unwittingly roam around in the spirit of the Festive Season and are vulnerable to likely offenders. Crimes of identity theft and fraud are thus highly likely to occur at this time of year.

5.2.2.1 ID Theft with the Intention of Opening False Accounts

The most common type of identity theft that was mentioned by the participants was the theft of identity documents for the purpose of opening false accounts. Below are the direct responses of the participants when asked about the most common form of identity theft and fraud:

P2: *"Stealing of ID's to open accounts [and to] take out loans and claims with the Road Accident Fund."*

P4: *"Identity document theft, where you find a victim has lost their ID. Perpetrators use victims' details which include their ID number, name, surname and date of birth.*

P5: *"Stealing of IDs and opening accounts. Some even go to the extent of buying houses and cars using your ID."*

P6: *"Opening of false accounts, bank accounts to commit fraud. They submit false company documentation. Opening of accounts in other people's names in order to misuse the account. Stealing another person's identity in order to seize their intellectual property or their Facebook accounts. There's a lot of Internet fraud currently occurring. Hacking of people's emails and impersonating the owner of the email in order to commit fraud."*

The respondents all agreed that ID document theft was the most prevalent of identity theft incidences. It is notable that this information was shared by participants who worked on different floors in the Unit and who specialised in different types of commercial crime. Some specialised in corruption while others dealt with fraud cases. It was also evident that the common goal of ID theft is to gain financially. This concurs with the rational choice theory which proposes that criminal

behaviour is rational and purposive (Cornish and Clarke, 2016:32). The respondents strongly illustrated the rationality behind identity theft that "crimes are purposive and deliberate acts, committed with the intention of benefiting the offender" (Ibid.). Wortely and Townsley (2016:33) state that identity thieves are perceived as rational beings due to the advancement in their execution of criminal events. This statement is congruent with the participants' responses that hacking, purchasing houses and cars (which are large investments), as well as the theft of IDs for the purpose of opening false accounts or for committing fraud are rife. From the latter one can deduce that these criminal behaviours exhibit technological advancement in the methods utilised by perpetrators to successfully execute the above. It is undeniable that most of these criminal acts are highly technical in nature, are serious, and involve large sums of money. These actions and intentions of perpetrators are not only as stipulated by the RCT, but are also supported by the literature, which reveals various types of identity theft, particularly cybercrime. This crime is prominent on SABRICS's current list of common crimes (South African Banking Risk Centre, 2019).

5.2.2.2 Prevalence of Fraudulent Marriages among Foreign Nationals

The prevalence of fraudulent marriages was identified as important due to the recurrence of this phenomenon, particularly as foreign nationals were identified as perpetrators of this crime over the many years that some participants had been working in the SCCU. Below are the views of a participant on the prevalence of fraudulent marriages, particularly amongst Pakistani nationals:

P1: *"[It is] prevalent mostly amongst foreign nationals, Pakistanis. They steal identity documents usually belonging to Indian women. They do so as to lower or eliminate any form of suspicion due to the colour of their skin. Whereas marriage between a Pakistani and a Black African woman will raise concern and suspicion and result in maybe further investigation by the marriage officiator such as the Department of Home Affairs. Victims of identity theft pertaining to fraudulent marriages are rife in Phoenix. This is because a large number of the Indian community is found in Phoenix."*

It may be argued that this finding indicates the need for awareness campaigns to normalise the targeting of specific ethnic groups in efforts to create awareness and mindfulness of such criminal

acts. This should not be shunned due to the possibility of viewing this as a form of racism. ID theft is associated with all types of fraudulent acts because, when perpetrators get hold of a victim's ID, they may commit a number of different types of fraud, of which fraudulent marriage is only one. Chapter 2 of the POPI Act No. 4 of 2013 (Republic of South Africa, 2013) opposes and outlaws the theft of information that is identifiable to a specific person, more so for inappropriate and illegal use. This act protects the privacy of all people, companies and organisations. According Botha, Swart and Eloff (2015:4), perpetrators who proceed in contradicting this Act, and those who are apprehended and found guilty, can be fined up to R10 million while they may also be sentenced to jail. The prevalence of fraudulent marriages as narrated by P1 can be associated with negligence and poor implementation of guiding rules and protocols in marital affairs and processes. It was therefore pleasing to read of Minister Aaron Mostoaledi's adamant determination that the DHA should prevent fraudulent marriages and take concerted steps to revoke the citizenship of foreign nationals who have committed the act of identity theft and fraud (Fokazi, 2020:1). The Minister further proposed the prohibition of marriages by the Department from occurring in absentia of the spouse, and urged the requirement that both parties must be present in order to consent to the marriage (Fokazi, 2020:1). In light of the above statements by the Minister, the regulation and monitoring of statistics based on incidences of fraudulent marriages by foreign nationals should be prioritised so that this picture may become clear.

5.2.2.3 Interception of Digital Money Transfers

Criminal behaviour that involves the digital interception of financial transactions reiterates the advanced and seriousness of the methods facilitated by identity theft and fraud perpetrators. Below is a response from a participant indicating the online interception of IDs, qualifications, and money transfers by perpetrators:

P2: *"The most common form that we receive is the stealing and use of another individual's qualification for the purpose of employment. Foreign nationals then commit fraud for the purpose of accessing social grants and or a pension fund. They do this by stealing an identity document belonging to another person and use it to access the above. Another common form of fraud that we as a Unit receive cases on is, the intercepting of money transfers... [Say] you're selling a house, and you're expecting to receive an amount of R1 million into your account. The perpetrator then*

intercepts an email that the buyer is about to receive and changes the account details of the individual who is supposed to receive the transferred money. The buyer will then receive the account number as listed by the perpetrator, with the money then going into the perpetrator's account. The email does not look suspicious as it entails the bank's details and stamp of approval. The buyer will receive this email as if it were from the selling individual's bank. They may intercept the email from the seller to the buyer, change the account details, and forward the email to the buyer. The seller may call to check with the buyer if they received the email sent by them. The buyer will then confirm having received the email without any suspicion."

Fraudulent acts committed by some foreign nationals are not limited to fraudulent marriages, but also include the interception of money transfers to gain access to social grants and even jobs. The perpetrator steals an ID in order to apply and become a social grant recipient while qualifications are fraudulently acquired to access high paying jobs.

Similar to P2's response, P8 had the following to say regarding the soliciting of information that enables the perpetrator to commit fraudulent acts:

P8: *"Perpetrators may intercept information. For example, a person opens an account at a clothing store. They submit all the required documentation. They go on to using their account by purchasing clothes. Soon after that they find out that they purchased items at Makro. The victim is surprised by this because they know they did not open an account nor did they lose their ID for someone else to then maybe open an account at Makro. This then means identity theft syndicates intercepted the information that was given by the victim to the clothing store, and were able to get the victim's personal and important information enabling them to open another account at a different store."*

The interception of a financial transfer and information communicated through email and by telephone requires a heightened level of technology. The ability and knowledge to commit the above acts of crime demand that perpetrators are not only able to carry out the criminal act, but that they do so while avoiding detection and apprehension. According to Grobler and Louwrens (2009:17), it is not only criminals who are responsible for Internet interceptions, but business competitors do this as well in the form of employees who launch cyberattacks against their

business rivals (Van Niekerk, 2017:3). P2 and P8 agreed, although they made reference to different monetary losses in the cases they mentioned. One can infer that these examples point out that the interception of money transfers may occur at any given time and without a specific transfer being targeted. Thus any online money transfer can be intercepted and hacked. It is therefore important that banks and similar organisations monitor and regulate large money transfers in order to ensure that transfers are not intercepted. However, this may be different for stores that utilise online platforms to sell their products. Having said this, the above is not an excuse for any breaches that occur, as the use of the Internet by various stores should be guided by and facilitated only upon the implementation of secure money transfers and ensured confidentiality of customer information. "The Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA), which was promulgated in 2002, regulates the interception of certain telephonic as well as Internet communications" (Katuu and Ngoepe, 2015:61). RICA (Republic of South Africa, 2002b) prohibits the interception of all forms of communication. This prohibition is thus not limited to the Internet and emails, but includes banking institutions, companies, and all other data breaches. Based on the aforementioned observations, one can deduce that this should caution and alert cybercrime units (CIUs) and the SCCU that perpetrators of fraud can be found in the least expected contexts. So, just as like anyone can fall victim to cybercrime and identity theft, anyone can be a perpetrator of such crimes.

5.2.2.4 ID Theft of Trademarks to Manufacture Counterfeit Goods

Amongst the most prevalent types of identity theft crimes is identity theft to manufacture counterfeit goods. P2 explained in detail how these actions are conducted and further detailed the apprehension of these perpetrators:

P2: *"Identity theft goes as far as counterfeit goods and or parts. For example, a company will start manufacturing Nike wear or goods. That company has stolen the identity of Nike. A consignment may come in from maybe India or China. When it arrives at the Durban harbour, it is inspected by the police, who then find Nike goods in the container. The police will then call Nike Head Office to inquire about the arriving shipment. To their surprise, they find that Nike was not expecting a shipment. Nike will then send one of their employees to inspect the arriving stock, only to find that the stock does not belong to them. So the unknown manufacturing company has stolen*

Nike's identity and manufactured a fraudulent product. Nike will then open a case, resulting in the arriving consignment being confiscated by the authorities. SCCU will then begin an investigation to find the perpetrators. The perpetrators are arrested on grounds of having stolen another company's identity and trademark. Such theft and fraud include products such as tablets [e.g., Disprin]. People manufacture and sell high demand tablets, water, cold drinks, cigarettes, and many other commonly desired goods. Perpetrators of such crimes are caught when customers start showing signs of food poisoning or they use certain tablets yet still feel ill. SCCU investigates and focuses on such cases. The reason is that such perpetration affects the country's economy, public health with people contracting different kinds of diseases due to food manufactured poorly by fraudulent manufacturing companies. When these perpetrators are caught and arrested, it may not necessarily mean the end of the manufacturing of that counterfeit goods or product. This is so as only the perpetrators that were supplying a certain place with water, for example UKZN, may be caught. The consignment might be supplied to the whole of KZN. So [if it is intercepted only here] the supply continues in other parts of the province. [It is] important to note, counterfeit goods are only investigated if and when a victim reports it. For example, one finds a snail in their bottled water, or bought expired food, or ate a certain type of food that resulted in food poisoning. Perpetrators are arrested and charged with serious fraud. They have negatively impacted and affected the economy and caused financial damage to the original owner of the brand."

In view of the above, it is clear that the manufacturing and selling of counterfeit goods have occurred for some time. This crime can be defined as the reproduction and recreation of a good, reputable product without the permission or authorisation of the legal owner for the purpose of gaining a profit (Reichel and Albanese, 2013:101). The information relayed by P2 depicts years of experience in dealing with the selling and manufacturing of counterfeit goods. More importantly, the investigating officer's emphasis on and knowledge of this matter exhibited the prevalence of this criminal behaviour. P2 described the perpetrators of counterfeit goods as identity thieves as he likened their actions to those of identity theft perpetrators. This participant also claimed that such perpetrators steal the identity/trademark of another company and then manufacture a counterfeit product under the identity of the original owner, and therefore he qualified this act as identity theft. Act No. 37 of 1997, namely the Counterfeit Goods Act (Republic of South Africa, 1997) prohibits the manufacturing, production and selling of counterfeit goods in South Africa

(Thenga 2020:11). P2's response is supported by an article by Naidoo (2019) in which it is stated that South Africa suffered more than R277 million due to counterfeit goods. The disturbing news was delivered by the Minister of Police at a conference that was held in Cape Town in October 2019.

Contrary to the existence of the above legislation, identity theft and fraud syndicates still continue to manufacture, produce and distribute counterfeit goods. "Authentic brand name goods are delivered to state owned or foreign owned stores through formal channels, [and] counterfeit goods flow into open-air wholesale markets located in densely populated areas that can be easily accessed by public transportation" (Lin, 2011:2). Based on this fact, if it is indeed how the production and sale of such products operate, it begs the question why the prevalence and transportation of counterfeit goods continue without detection or eradication. The main reason for research in the Criminology field is to elicit information that can ultimately lead to the deterrence of criminal perpetration. Therefore, with access to such information and knowledge as mentioned by Lin (2011), the researcher is of the view that figures of incidences of this sort should be seen as efforts to deter such crimes, as they reveal that a blind eye has not been turned to such criminal acts.

5.2.3 Potential Victims of ID Theft and Fraud

Anderson (2005:12) lists various characteristics that are influential in terms of who become victims of identity theft. The data that were obtained in this regard concurred with the literature. For instance, the United States Department of Justice (2012:8) postulates that identity theft is an equal opportunity crime as it is not specific to gender, ethnicity, marital status or age – rather, any individual is at risk of becoming a victim of identity theft. When asked what caused one to be a potential victim of identity theft and fraud, the participants responded as follows:

P9: *"Greediness, carelessness or negligence of victims. Victims sometimes lose their bags and in them they have important documents which they maybe did not even need to have with them."*

P10: *"It's mostly caused by negligence of victims who are scammed. Victims wanting something that will generate money quicker compared to a monthly salary which puts them at risk and makes them vulnerable to fraud."*

In contrast to the above responses by P9 and P10, P2, who had years of experience in the SCCU, stated the following:

P2: *"Half the products you see and that are manufactured and sold on the streets are counterfeit. The chemicals and everything else that were used to manufacture these products are mostly unworthy of being used or sold to people."*

The information provided above can be aligned with the participants' experiences of commercial crime investigations, and further accentuates the importance of regarding and recording, whether statistically or in literature text, the ever changing modus operandi (MO) of perpetrators. Based on the above response by P2, one can argue that, contrary to the notion of a single individual potentially being a victim of identity theft, any individual, company and organisation is prone to their identity being stolen and misused for financial gain. Based on P2's years' of experience in the force, he alluded to the fact that identity theft and fraud are not limited to an individual's identity, as they also investigated cases of manufacturing and selling of counterfeit goods. This highlights the point that using a trademark that belongs to another as your own can be classified as a form of identity theft.

Victim vulnerability makes anyone a potential victim of identity theft. As stipulated by P10, certain individuals of identity theft and fraud find themselves in this kind of predicament due to, for instance, dissatisfaction with their monthly salary. The researcher believes that this may be due to incomes that are below some individuals' living expenses, while others are victimised purely because of greed. The latter point was supported by P9, who mentioned greed as one of the elements that lead to victimisation. This then results in the fact that many individuals fall victim to scams and fraud. Based on the latter, one can deduce that the possibility of falling victim to fraud does not only depend on gender, ethnicity, marital status, age, and income (Anderson, 2005:12), but that any person, company, and organisation can be a victim of identity theft.

Contrary to the notion of the negligence of victims as referred to above, RAT states that one is at a greater risk of becoming a victim of theft in the absence of capable guardianship and the presence of a likely offender (Cohen and Felson, 1979). The issue of negligence then becomes questionable when the aforementioned characteristics of RAT are considered in cases where individuals fall

victim to theft when a bag and or purse is grabbed by a perpetrator. In light of the latter, one can argue that the responsibility of this unfortunate incident cannot solely be attributed to negligence on the part of the victim. The applicability of RAT was also supported in a response by P2, who noted the prevalence of the theft of companies' and persons' trademarks. One can again argue that this cannot be associated with negligence by the victim, but rather the absence of capable guarding and preventative channels to ensure that the above does not occur. With reference to the points that were highlighted above, the researcher identified a loophole with regards to strategies in place to govern and police the safety of South African citizens that is used by identity theft perpetrators. In view of the foregoing, one can deduce that, because such individuals and syndicates are incessantly on the lookout for opportunities to perpetrate theft in the absence of capable guardianship measures, creative strategies should be devised and supported by regulations to ensure guardianships that prevent such ruthless perpetrators from operating.

5.2.4 Causes of Identity Theft and Fraud: Are Identity Theft Perpetrators Rational Beings?

As explained by Burke (2018:8), the purpose of utilising a theory is not to conduct further research on the theory itself, but rather to support, refute, or question certain findings. In support of this statement, the following responses regarding the causes of identity theft and fraud were analysed with reference to the adopted theories:

P2: *"There are various reasons why perpetrators commit identity theft. New opportunities are found by perpetrators. The discovery of information that they previously did not have, but mostly it is caused by greed. As a country we are divided into two sub categories, one part being affluent and the other living just above and the others below average. The majority of those who are on the opposite side of the affluent want and desire the livelihood of those that are well off. Therefore, they commit identity theft for the purpose of fraudulent acts that will result in them having a portion or more of what the affluent have. It would maybe be different if we all lived on the same breadline, but for such perpetrators and the poor they are not blind to those that are wealthy as we all live where we can see how others live. Mostly it is due to the country's structural economy. The poor desire and feel the need to have what the affluent have, and will see such a life as within their grasp and accessible to them. Foreign nationals who come to South Africa see this as a land of opportunities, hence they utilise those opportunities by mostly illegal means."*

In contrast to the above in-depth response by P2, the other investigating officers had the following to say:

P4: *"Perpetrators are greedy for money."*

P6: *"Pure greed! Identity thieves work to manipulate people using or impersonating others or under a false identity. People do not want to work properly for money."*

P7: *"Greed, with some being born with criminality or criminal traits. Some we find are employed but they still commit fraud. You start to notice the things they own which are far more than what their salary can afford. [Also] peer pressure, where we find that friends will teach them or ask how they make money and they see it as extra cash that comes easily."*

P9: *"Money! People want money and assets. Greediness."*

It is evident from the above responses that the socio-economic challenges that some perpetrators face influence their criminal tendency. In light of this, the researcher infers that such challenges may be associated with social injustices that existed for a long time and that have ultimately affected many generations, thus leading to different reactions and responses, with crime being amongst them. P2 inferred that many criminally-minded people tend to desire the material and financial freedom that exists and that is within their sight, and that these people are not blind to the life enjoyed by the wealthy. However, this does not justify their criminal actions.

Criminal behaviour is not only associated with perpetrators from poor economic backgrounds, but with the wealthy and well-off as well. This notion was supported by P6 and P7 who stipulated that some people are merely greedy and that their actions are not based on socio-economic injustices or issues, but rather on the desire to live beyond their current means. In this context, their criminal behaviour is purposive and rational. To explain this finding in depth, RCT's third concept applies, which stipulates that criminal decision making is crime specific (Cornish and Clarke, 2016:34). According to this theory, it is important to examine the motive behind different criminal behaviours, as decision making pertaining to each criminal event differs from that of others. One can thus deduce that the importance of examining and addressing the decisions that lead to a particular type of criminal event, such as socio-economic inequalities, should not be negated as they generate and drive the root causes of crime, and such knowledge will assist in combating and preventing further criminal behaviour in a particular criminal context.

5.3 Preventative Measures for ID Theft and Fraud

5.3.1 Procedural Mandate of the SCCU

Risk assessment strategies are imperative to prevent criminal activities. In cases where perpetrators initiate criminal activity, these strategies also help to render them unsuccessful due to the interception of their plan by a risk identifying system. The following responses were offered when the participants were asked if they were aware of risk assessment strategies and if these were in place should any threats of identity theft and fraud transpire:

P1: *"The monitoring and assessing of risks in order to identify emerging risks is facilitated by other units such as Crime Intelligence (CI), not the SCCU."*

P2: *"There is a standardised Department that deals with such work of identifying current and emerging risks known as the Criminal Intelligence Unit (CIU). It is a unit that was designed to be a collector of information. We at times task the CIU for information when dealing with cases of fraud."*

P6: *"Uhm, in the Commercial Branch it is what one would refer to as reactive investigations, so you receive a complaint or docket."*

P10: *"The Crime Office is responsible for identifying current and emerging risks. The Crime Unit is a unit that analyses crime and checks the different patterns of crime and follows trends. For example, if perpetrators are used to scam ATMs on Fridays at a certain time, and then this changes due to maybe police officials being deployed to monitor that area. Employees at the Crime Office will then pick up the above changes and notify Management who then deploys officers to the syndicate's new area and sensitises the public."*

P11: *"We have an MIC Office that is responsible for identifying and monitoring what crimes happen in which areas and they then concentrate on those areas to combat crime. We also have a BCNC Office, where all of the cases go to, and they can then see and identify the area where maybe identity theft is occurring and they concentrate on that area. We have entities within the police as well SABRIC, where all cases go through to them, including banks, and they send out a report on a monthly basis, stipulating different crimes and where they occurred."*

The participants' responses were analogous to a large extent, as they stipulated that the SCCU is not responsible for identifying risks but rather handles cases that police stations can no longer investigate due to insufficient resources. Such cases require extensive periods of time, skill and intelligence. This notion was supported by P1 and P2. According to the latter respondent, the CIU is responsible for identifying and measuring any risk and threat that might impact the public. Some cases are known as reactive investigations, as in these cases the unit receives a docket concerning a case that was active but not resolved, which is then referred to the SCCU. P11's response referred to the collaborative manner in which crime prevention operates as it is inclusive of various bodies that play different roles. In light of the above, one can deduce that it is necessary that all entities, inter alia the MIC office, the BCNC office, as well as SABRIC, are in constant communication with one another in order to deter and combat crime. Although a tad different from P11's response, P10 concurred in essence with the statement about the need for communication amongst entities. The latter participant also stated that the Crime Office, which is responsible for monitoring crime trends, relays any information regarding new crime. Upon communicating new crime trends as well as the area in which they seem to occur, police officers are then deployed to that area. It seemed that only a few participants possessed extensive experience and knowledge of other units apart from the one in which they worked. These were units that they contacted at times to source crime information.

5.3.1.1 Response to the Call to Curb ID Theft and Fraud by the SCCU

When asking each respondent how they measured and determined strategies to yield positive results in their investigations, the following comments and insights were offered:

P1: *"Every case is result driven. When conducting an investigation when a crime was committed, at the end of the day someone must be arrested, prosecuted and sent to prison. When the investigation has proved and concluded that a perpetrator did indeed commit a crime, the unit is able to say that the investigation was successfully and properly done. With the perpetrator being arrested and convicted."*

P3: *"If you are able to trace back a suspect using the evidence collected."*

The researcher probed: "*So you determine effectiveness using the number of arrests made?"*

P3: *Yes, because if there is a high detection rate, one is able to say that work is being successfully carried out. Cases that go unsolved or undetected in our part as a Unit inform us that there is a lot more work to be done. There is a high rate of fraud."*

P4: *"The only way to determine if the investigation was successful is if I make an arrest."*

P6: *"The SAPS receives dockets that we're required to go through and understand what the complaint is or what the case is about, and you set out an investigation plan that will give an idea of which way you will go about investigating a case. With any investigation one has to be open minded; one can't investigate something with a one- sided approach or way of thinking. You don't make a decision before you've seen and collected all the evidence. You have to be impartial during an investigation, you can't be told by one person that the other is a bad person, then make a decision that what was said is true. You don't take things at face value. You have to be fair to everyone involved, both the complainant and the accused. Now and again there are people who try to mislead you or a case and give you false information, pointing fingers at another person. SAPS SCCU is very much governed by the law. We have to follow certain procedures and we have to adhere to the rules set when dealing with cases of counterfeit goods fraud. Gather and find as much information as you can and don't rely on one piece of information to solve a matter. In terms of fraud, mostly documentation would be what an investigator looks out for, which includes bank accounts that are important."*

P7: *"During an investigation, in the process of taking statements one can tell if a case is going well. As an investigating officer I meet with the prosecutor and discuss what needs to be done. We go out to collect more evidence. We then put our work together and when it's enough to make an arrest, we do so. When a suspect is arrested and he is someone who is resourceful, sophisticated and has committed such criminal acts in various places, we oppose bail. In some cases, we drop the investigation if, after months of investigation, we have no positive output."*

P8: *"You look or calculate productivity. You look at your* ***output****. Complaints that are coming in would be the* ***input****. If, out of ten cases you solve three and the other seven remain unsolved, you can then say you are at a 30% performance with regards to solving that particular category of crime. Crime categories are not the same. We have performance assessments that measure each and every crime code. Which then stipulates that within that jurisdiction so many cases have been*

reported, a certain number has been solved, and a certain number was not solved. [In the] Justice System there are also other research councils, that may assist."

The researcher probed: "*Does it happen that a criminal's MO was only known of or about after a crime has occurred?*

P8: "*Sometimes you know of a crime because a complainant came in and reported it. Within SAPS there is a structure or unit known as Crime Intelligence. They are tasked with identifying crime either before or after it has occurred. But with regards to identity theft and fraud, they can only identify or detect it after it has been committed. They may identify patterns and trends."*
P9: *"Investigators normally have various investigating plans that they can follow and will attempt various methods and or processes that will eventually lead to them making an arrest."*
P10: *"By making an arrest and the perpetrator is sentenced, and you do so without being required to conduct a further investigation due to loopholes being identified. Loopholes may occur if an IO did not explain the perpetrator's rights, which may end up jeopardising the case."*
P11: *"Through your detection rate. We have an SAP6. If you have a conviction it goes on the SAP6, and it is calculated mathematically and it calculates your detection rate. SAP6 is not only for identity theft, it's for different dockets that you carry and work on."*

The focus of the study was to explore the policing of identity theft. It was thus pivotal to question how the Unit determined the effectiveness of their policing and investigative strategies. Although the responses differed and exposed various elements pertinent to this exploration, most understood that there was some measurement of their successes in resolving cases. For instance, P1, P4, P9 and P10 concurred that the effectiveness of their strategies was determined by making an arrest.

The analysis suggests that there is no single method or procedure of investigating a case in this crime category. This notion was supported clearly by P6, who propagated the importance of 'open mindedness' and avoiding a one-sided approach during investigations. P9 concurred by stipulating that there are various methods that investigating officers ascribe to and attempt that may ultimately lead to the arrest of the perpetrator. The latter is evidence of and highlights the extensive amount of work that investigating officers do when dealing with cases of identity theft and fraud. Another

conclusion in terms of investigating procedures is that some methods seem to rely on trial and error until a successful conclusion is reached. As was stated, such cases may lag for months on end with no success of arrests. This results in the fact that such cases are dropped and the investigation is abolished. In view of this, it may be deduced that disadvantages of the trial and error approach are the time required to address such cases of fraud, and that this gives the perpetrator time to relocate and commit the crime elsewhere.

5.3.1.2 Measures Taken upon Discovering ID Theft and Fraud by the SCCU

The participants agreed that a victim's location upon discovery of being victimised determines where the victim should open a case of identity theft. The victim's first course of action is to report this act and the point of contact is the nearest police station. Below are participants' responses based on the measures that should be taken by a victim upon discovery of the theft of the ID or other documents and money:

P2: *"The point of entry is the police station. The victim will visit their nearest police station and lay a complaint. The case is opened and investigated by the station. If, after an in-depth investigation, the investigator finds the case to be more complex and in need of specialists who specialise in such cases of stolen identity and fraud, the case will then be sent or referred to the Commercial Crime Unit."*

P3: *"A victim of fraud reports and opens a case at a police station. Depending on the loss suffered by the victim, if it is more than R500 000, that docket is sent to SCCU to be investigated by this Unit. Some perpetrators are caught while others are never caught. One of the reasons of failure to catch and arrest perpetrators is that some will reside in a certain location which is frequented by many people, for example the Durban central business area. After the perpetrator has made their gain, they then move back to their original location or find a new place."*

P4: *"Most of the time the victim has to first report to their nearest police station. The minute a person becomes aware that they have lost their ID, whether they are not sure if anything has been done or their ID has been used somewhere, they should report the matter at the police station and write a statement. This assists a person when and if something happens in the future, such as the theft of their identity for the purpose of fraud. Then the victim can be able to report and show proof (the statement) that they reported losing their ID. This helps a victim a lot."*

P5: *"The victim must first go to their nearest police station and open a case, have a case number then go to the places where the suspect/perpetrator committed fraud using their personal details."*

P6: *"The stores themselves cannot help a victim of fraud or theft. A victim can go to the police station, and lay a complaint at the charge office and open up a case. Victims may also go to an attorney, and take a civil route. Although that will obviously cost the victim a lot of money. There's a fine line between civil and criminal when dealing with matters of fraud. So you rarely find people who look for the assistance of an attorney."*

P7: *"The victim approaches their nearest police station, writes a statement, and makes an Affidavit after discovering the loss of their ID. If the victim finds out during an investigation that they have been a victim of ID theft and fraud, they are required to then open a case if they claim to be innocent or unaware of any illegal transactions and activities done in their name".*

P8: *"You go to a police station depending on the information available. If you lost your ID at home and you're sure you lost or misplaced it at home or it was stolen at your home, you report the theft of an ID at the police station. You then later find out that your ID has been used in Cape Town, a case of fraud will then be opened in Cape Town. The victim then becomes a witness to that case of fraud and will submit the initial report or statement that the victim wrote when they discovered the loss of their ID. All these documents will then be sent to Cape Town."*

P9: *"The victim can go to the police station. The minute a person loses their ID or when they realise that they have lost it, they must report the matter at the police station, before it is even used illegally by a perpetrator. The same goes for a bank card or store account. A person must report at the relevant store or institution. Or Home Affairs, if you have lost your ID. School, if you lost your qualification certificate."*

P10: *"You got to the police station and open a case just like any other case. The docket will then be allocated to the Fraud Unit. Depending on the value of the case, if it's below R500 000 it will be sent to the Provincial Commercial Crime Unit, if the value is above R500 000 it will be sent to SAPS SCCU, 14th floor. If it is a high profile case, involving for example a minister with a political affiliation, it is sent directly to SAPS SCCU. External role players, PIPA hotline, etc."*

P11: *"The victim is to go to any police station. There are also websites such as SABRIC that you can logon to, which have a lot of information on identity theft. It may also be reported to the Department of Home Affairs, or the bank if the victims' bank account was compromised."*

The participants shared the view that it is important to report identity theft and fraud cases, stating that cases should be opened at the victims nearest police station. Some further emphasised that cases are only sent to the SCCU if the monetary value suffered exceeds R500 000, if the complexity of the case demands deeper investigation, or if there are inadequate resources at the local police station to further investigate the case.

However, the researcher discovered that a gap exists in the literature within the South African context as the literature review revealed a dearth of information regarding the measures victims should take upon the discovery of having fallen victim to identity theft. Due to this gap, the researcher relied on international literature to illuminate this matter in Chapter two. In light of this gap, the participants' responses regarding the process victims should follow when reporting cases of identity theft and fraud were thus imperative in enhancing the findings of this study.

What the researcher wishes to highlight as a pivotal element in the working relationship between local police stations and the SCCU is the communication of information regarding developments in a case. One may thus infer that, should a case be transferred to the SCCU, it is incumbent that the authorities (i.e., the investigating officer) should notify the victim. Furthermore, victims should never be in a position where they are marginalised due to a lack of progress in a case. Based on the latter, priority must be given to clearing the victim if s/he is indeed innocent as opposed to finding the suspect or perpetrator. This is particularly important due to the extent of time such investigations may go on for. Assisting the victim and ensuring that s/he is indeed innocent will give them the opportunity to continue with their lives whilst investigations to find the offender/s are under way.

5.3.2 Usefulness of an Automated Identification System

The human identification theory, which has very little to no support in published research, has a rather large impact on explanations of the preventative measures that should be taken against different crimes − in this case identity theft and fraud. Below are participants' responses relating to the use of an automated identification system by the Department of Home Affairs (DHA):

P1: *"A woman was caught at the DHA when the photo appearing on the ID did not match the photo that they had on their system."*

P1: *"Identity theft perpetrators are known to steal identity documents. They then remove the original owner's photo, and replace it with their own photo, thus creating a misrepresentation of the details on the ID and the photo appearing on the document. This then allows them to present this ID in various places when required to do so. Person(s) receiving the ID presented by the perpetrator assume without question that the person appearing on the ID is in actual fact the owner. Trouble starts when the document is presented at Home Affairs. The ID number is entered on the system and shows all the details of the owner of the ID number. The Home Affairs official then notices any irregularities such as the different pictures that then appear."*

P5: *"Identity theft investigations mostly involve being in contact with and working with Home Affairs. So at times you will request their assistance on a case and the process may take time. It's usually a long process."*

P11: *"Yes, we have to work with other departments in these cases to catch perpetrators. It's very important because that's how you find information and get assistance."*

The proponents of this theory have seen departments, such as Home Affairs, facilitate and utilise an automated system (HANIS) which allows South African citizens to be assisted should they become victims of identity theft (see Chapter Two) (Cassim, 2015:). Although some may argue that this system is only helpful when it comes into play after the commission of a crime, the use of an automated system by the DHA was supported by a participant who elaborated on the role played by the DHA in the case of a stolen ID. According P1, the DHA uses an individual's biometrics, or physical characteristics, that include fingerprints, retinal scan, a physical description, the DNA pattern, and the signature of a person (Lo Plucki, 2008:8). It can thus be deduced that a physical description and the use of fingerprints by the DHA, as well as any other institution, lower the risk of identity theft and fraud. One can further infer that although some perpetrators may commit the act of fraud through identity theft, the chances of them being caught when there is an automated system in place are a lot higher than in a purely manual system.

In view of the above, the initiation of an automated system is commendable and has proven to be of assistance, as was mentioned by the latter participant. However, the numbers of identity theft and fraud cases are still quite high and rising, and therefore more should be done to decrease the

occurrence of such cases. Primarily, loopholes must be identified as thieves tend to find ways around security systems. In some cases, as was mentioned by the participants, employees themselves may have been recruited by larger syndicates and they then use their position in companies or organisations to commit identity theft and fraud. It is thus crucial that investigative units such as the SCCU and Departments such as the DHA question how, amidst already existing preventive systems, thieves still manage to conduct their criminal acts. All affected organisations and bodies should ultimately develop a plan of action and strategies to better deal with incidences of identity theft and fraud.

5.3.3 Awareness Campaigns as a Preventative Measure

It was stipulated by most participants when they were asked about preventative measures and strategies that the citizenry has to be sensitised to this crime. They mentioned the following regarding awareness campaigns:

P1: *"Conscientise and teach people about the different crimes that can be committed using their IDs. I have noticed that people want to learn after the fact and thus the hard way."*

P3: *"We hold fraud awareness campaigns where we educate and warn people not to take their money and invest it in pyramid schemes. We inform them to research and visit recognised banking institutions with FCP numbers where it is safe to invest money."*

P7: *"Awareness campaigns, although these are not enough as there are too many people out there. SAPS SCCU is the only unit in KZN that specialises in fraud cases. SAPS officials, particularly those in communities should be aware of and deal with fraud in order to conscientise the community of new trends. The outskirts need more police officials, because you find that perpetrators soon move away from committing crime in CBDs as there are a lot of SAPS dispersed in such areas."*

P8: *"Awareness campaigns. Through radio, publications, online, social media. But you can only go that far, because you cannot police victims on how to behave, but you can conscientise them."*

P10: *"Sensitising people by conducting of awareness campaigns through different radio stations in order to cover all language spectrums. Particularly reaching those in rural areas because they are mostly targeted by fraudsters due to lack of knowledge. Therefore, a visit by an employee from the Communication Department, a Communication Officer who will sensitise listeners. Awareness*

campaigns where Communication Officers will go directly into the community and sensitise people. Conducting awareness campaigns in order to sensitise people to be alert and take precautionary security measures when and where they can."

In line with the above responses, the routine activity theory (RAT) argues that a likely offender may also be a perpetrator who does not necessarily come in direct physical contact with a victim, but may use online platforms. An analysis of the above responses, which were in agreement at a rate of more than 50%, begs the question whether awareness campaigns are truly the only medium to ensure protection against identity theft and fraud. P7's comment is notable as this respondent argued for the importance of awareness campaigns, but further postulated that criminals tend to move to the outskirts where there are few or no police officials nearby, which necessitates the deployment of police officials in such areas. Such officers' reports can then contribute to crime statistics in the case of identity theft and fraud. Crime in areas located in and around CBDs can be identified and reported due to a large dispersion of police officials in these areas. This is opposed to the outskirts where crime may not even be reported due to a lack of SAPS presence in these communities. This notion was supported by P10, who argued that awareness campaigns in communities located on the outskirts are particularly important as these areas are targeted by perpetrators due to these citizens' limited knowledge regarding crime in general and identity theft and fraud in particular. The importance of awareness campaigns that was highlighted by all the participants as a preventative method cannot be denied. Therefore, drawing from RAT, it seems urgent that a strategy needs to be devised to ensure the presence of at least a minimal amount of 'capable guardians' in these outlying areas, as they will be instrumental in decreasing the victimisation of these communities not only in terms of ID theft and fraud, but other crimes as well.

5.4 Challenges Experienced by the SCCU in Response to and Prevention of ID Theft and Fraud

Below are the themes that emerged when the participants were asked to comment on the challenges that they were confronted with when investigating cases of identity theft and fraud:

5.4.1 Overworked Staff Members by the SCCU in Response to and Prevention of ID Theft and Fraud.

The following comments were made that revealed the theme of inadequate resources and a too heavy workload, ultimately resulting in overworked staff members within the SCCU.

P2: *"There are a lot of challenges that law enforcement agencies as well the SCCU face. In the whole of KZN, SCCU on this floor is the only unit or department that deals with cases of identity theft using stolen trademarks. For example, steal the trademark belonging to the University of KwaZulu-Natal and print certificates and qualifications in exchange for money. This floor is the only floor that deals with such theft in the whole of KZN. Manpower is another issue that we face as a Unit. The reason for this is, in the past only a certain calibre of individuals qualified to work in the Commercial Crime Unit due to the skills and level of education required for this job. Most people then only reached Grade 12, and most of the people who applied and entered into policing were such individuals as police officials were mostly tasked with running after and catching criminals. Therefore, Grade 12 level of education and fitness were the criteria for entering into the police workforce. This is in contrast to units such as our own, which requires tertiary education qualifications with specialisation of the work being done in the SCCU. Since the type of people who entered this field were those with Grade 12, challenges regarding understanding of the work being done within the Unit became an issue. Although, with the new system that separates those who strictly qualify to work as police officials and those who studied further and specialised in certain fields, the SCCU and many other police units will benefit immensely. Cybercrime is a buzzword. Although crimes of identity theft and fraud are being committed through the use of technology, in South Africa cybercrime is still a buzzword as practically we are far behind in terms of structures in place to oversee and combat cybercrime.*

Understanding and further addressing the challenges faced by the SCCU is imperative to improving the working standards of the Unit. The issue of manpower that was raised by P2 is concurred by Frakes (2009:4), who states that previously all that was required of one to enter the police force was to shadow another police officer for a week or two. During this time one learned how to assist victims with opening cases and writing statements. Thus limited qualifications were necessary or required. As mentioned by P2, an individual only had to produce a Matric certificate to enter into the police force. Currently, this becomes a problem when dealing with cases such as identity theft and fraud, as such investigations demand a certain level of education and academic sophistication. Based on recent adjustments, all Units within the SAPS will now be assigned employees who have attained appropriate qualifications. The knowledge that P2 possessed attests to the years he spent in the CCU since the time when he had been recruited, which dated back to the time when recruits were not required to be in possession of a high level of education in order to enter the police force.

The lack of resources that was mentioned can also be associated with the issue of manpower. However, it is surmised that, by means of a new employment strategy that was referred to according to which suitably qualified individuals will be recruited, the Unit will be able to deal with and manage the number of cases sent to them from all over KwaZulu-Natal. In light of the challenges that were referred to, one can infer that they should be monitored against the number of cases resolved as well as the rate at which identity theft and fraud cases are solved. In view of the latter, it is thus of pivotal importance to address issues that confront protective units in order to minimise and eventually diminish any challenges that prohibit a heightened level of productivity. The main objective is to manoeuvre towards a progressive and operational manner of working that will result in the desired improvement of prosecution rates.

5.4.2 Noncompliance by Implicated Organisations and Departments in ID Theft and Fraud Cases.

The participants were critical of the non-compliance by implicated institutions and departments when cases of fraud and identity theft were investigated. Below are two participants' responses in this regard:

P5: *"Identity theft investigation mostly involve being in contact with and working with Home Affairs. So at times you will request their assistance on a case and the process may take time. It's usually a long process."*

P9: *"Certain institutions that may be connected to or affected by the case are sometimes not willing to assist investigating officers. There is a lot of out-sourcing that goes into investigating such cases which makes the process take a really long time. Sometimes banks will instruct victims of identity fraud to go open a case with the SAPS instead of taking matters into their own hands and opening an inquiry or investigation as the victim is their client. They do this in order to avoid any legal or financial costs that may go into investigating the case. The process may be really long and frustrating for the victim to handle."*

The above comments describe the processes that take place during an identity theft and fraud investigation. What one can deduce is the importance of establishing partnerships with different departments and institutions that are connected to or are affected by cases of ID theft and fraud. The significance of the comments is that some organisations or companies fail to comply with evidence requirements and this hinders the progress of such investigations. P9 in particular argued that implicated institutions, instead of assisting and conducting internal investigations, will at times advise victims to open a case with the SAPS. According to P9 banks often do so in order to avoid accounting for any legal costs that are incurred by conducting such investigations. It is apparent that the time frame of investigations is extensive due to noncompliance, which is one of the many reasons that it takes so long to solve cases. Reluctance to comply is mostly associated with the fear of unravelling any shortcomings on the part of a department or organisation that may have contributed to ID exposure or made a victims' information easily accessible to the perpetrator. The comments of participants regarding working with other organisations during an investigation were indicative of a long and tedious process to solve such cases. This is exacerbated by the refusal of affected businesses or organisations to cooperate. P9 shared the feeling of frustration that victims are subjected to due to the extensive amount of time it takes to resolve an identity theft and fraud case. In light of the latter, one can infer that the stress experienced by victims may demotivate them from reporting or continuing with such cases due to the lagging and frustrating process that they have to endure. There should thus be compelling regulations that ensure the compliance of

such organisations and institutions as a lack thereof does not in any manner assist victims, nor ensure the timely apprehension of perpetrators.

5.4.3 Identifying the suspect

A third challenge that was referred to is the identification of a suspect:

P2: *"...a unit designed to be a collector of information. We at times task the CIU for information when dealing with cases of fraud."*

P6: *"Identification. Identifying the suspect, especially with modern technology [is difficult] as there are a lot of things that perpetrators can hide behind. There are laws in place that are not really policed properly."*

P8: *"The biggest challenge is identifying the perpetrator, because you don't have the perpetrator's identity. The only person's identity you have is the victim's...."*

Most participants mentioned that identifying a suspect in the case of identity theft for the purpose of fraud is quite challenging. This finding is intensely thought provoking and daunting in the light of modern technology and cybercrime. This notion was supported by P6 who argued that identifying a suspect is difficult, particularly with modern technology that enables the perpetrator to hide behind a laptop, PC, or cellular phone. The difficulty experienced in identifying the suspect concurs with the literature (see Chapter Two) concerning the advancements in technology known as high-frequency and high-technology crimes. P2 mentioned earlier that, in the event of a case requiring intelligence from for example the CIU, they requested assistance and tasked the Unit with the problem at hand. This emphasises the need for suitably qualified employees who have the ability to investigate, take on, and apply the intelligence demanded by such difficult cases of identity theft and fraud. For instance:

P4: *"A problem we face is that it is easier to identify the person whose ID was used to commit fraud than it is to find the suspect. In most cases, during an investigation, you will trace the transactions and purchases made by the suspect and find that he sold the car that he had bought using the victim's details. Details will easily point you to the victim of the crime who will state that they are not aware of any purchases made nor did she purchase a car. Another problem we face*

is that when a person purchases a car at Nissan through Absa Bank, you find that an employee at this company is part of and works with the perpetrator, which makes it harder and a tiring job to find the suspect. The individual who is supposed to check such transactions and report them, works in cahoots with the identity theft perpetrators."

It is important to note that P4 referred to the example of bank employees who are accomplices of identity theft and fraud syndicates. This fact, coupled with a bank authorities' reluctance to comply, make it very challenging to identify the suspect and perpetrators involved. This further derails the case and causes the investigation to be strenuous not only for the investigating officer tasked to resolve the case, but more so for victims who wait months on end for their name to be cleared. In view of the aforementioned, shedding light on issues and challenges faced by investigating officers when conducting investigations is pivotal in identifying hurdles that further prohibit the deterrence of identity theft and fraud. One can thus deduce that addressing the above challenges will be a step towards the deterrence of this crime. It will also ensure the enhanced productivity of investigators and a heightened level of success in the resolution of cases.

5.5 Conclusion

The corroboration among the participants' responses exhibited their in-depth knowledge about identity theft and fraud, although it was clear that some participants possessed more experience in this field than others. Contradictory to the figures listed (see Chapter Two) regarding the solution of the crime of ID theft and fraud, participants indicated that, although it takes months and even years to solve identity theft cases, they were quite successful in resolving such cases. However, the financial losses suffered due to ID theft is unacceptably high and therefore the successful resolution of some identity theft and fraud cases is commendable, but not sufficient. Civilians should not fall victim to identity theft and fraud, especially as waiting for such cases to be resolved is daunting and tedious. It needs to be iterated that there were discrepancies in the information provided by the respondents and the figures provided by organisations such as SABRIC (see Chapter One). This is attributed to the fact that members of the Unit under investigation are not tasked with all investigations concerning ID theft and fraud.

The above analysis looked at and recorded the different causes of the phenomena (ID theft and fraud) under study and the dreadful experiences that victims suffer due to ID theft victimisation. The discourse also examined the effectiveness of this Unit's efforts in policing identity theft and fraud. The analysis exposed some factors that prevent and inhibit the effective conclusion of such cases. The participants were in agreement that advancements in technology used by identity theft syndicates make it difficult for police investigative units to detect perpetrators and curb this crime. The challenges that affect the efficiency of the investigations were discussed, which included limited resources, heavy workloads, difficulty in tracing and identifying suspects due to highly sophisticated online systems, and non-compliance by implicated institutions. It is important to note these factors as they are concerns that hinder the smooth functioning and progress of ID theft and fraud investigations.

The chapter that follows will conclude this report by providing a detailed summary of the study and recapping the findings pertaining to the emerging themes. Recommendations based on the information that was imparted by the participants will be offered to curb identity theft. Finally, some guidelines will be offered for future studies in the policing of identity theft and fraud field.

CHAPTER SIX
CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter will provide a summary of the objectives the study sought to address. The themes that emerged will be discussed and recommendations will be offered for curbing identity theft and fraud. Lastly, propositions regarding future studies will be postulated. This research study examined and addressed all the research objectives that the study intended to explore. The primary objective, that formed the premise of the study, was to explore the procedural mandate followed by investigating officers and the challenges, if any, investigators experienced in policing identity theft and fraud. This objective was probed due to an incline in the number of ID thefts as well as the unpleasant experiences of victims of identity theft and fraud as observed in the literature. Upon addressing the questions that the study posed, various themes emerged that highlighted some of the issues that the investigating officers faced when conducting investigations of identity theft and fraud. Recommendations for resolving some of these issues will thus be offered in an effort to support efficient policing and investigative procedures that may lead to successful resolution of cases.

6.2 Objectives addressed in the study

The study findings were successful in addressing the following objectives:

- The nature and extent of identity theft and fraud in Durban, KwaZulu-Natal;
- The causes of identity theft and fraud in Durban;
- The effectiveness of the strategies employed by the SAPS SCCU in policing identity theft in Durban;
- The challenges experienced in the policing of identity theft in Durban; and
- Formulating recommendations for curbing identity theft in Durban.

6.3 General Conclusions

6.3.1 The nature and extent of identity theft and fraud in KZN, Durban

The research study found that the participants agreed on the nature and extent of identity theft in the study area due to their many years of experience in the Unit under study. In this regard, most of the participants agreed that this crime was prevalent but they could not confidently postulate as to the extent and exact figures, as cases are opened at local police stations and corresponding institutions with only some (those within their mandate) directed to the Unit for further investigation. Although the extent and severity of identity theft could not be precisely established, receiving detailed information about its existence was sufficient to warrant this in-depth examination of this phenomenon.

The nature of ID Theft and Fraud included, ID Theft with the Intention of opening false accounts, Fraudulent Marriages, Interception of Digital Money Transfers and the ID Theft of Trademarks to Manufacture Counterfeit goods. This information exude by participants indicates not only the nature thereof, but the extent of ID Theft and Fraud all around KZN, particularly Durban. Participants provided extensive intelligence, concerning the MO utilised by ID Theft and Fraud perpetrators in each of the aforementioned crimes. These ranged from low technology and/ traditional methods to high technology, further giving credence to the magnitude of ID Theft and Fraud.

The consequences of identity theft and fraud deny protective bodies, such as the SAPS, the opportunity to claim any ignorance of the existence and prevalence of this crime. The responses of the participants were unhesitating and they confirmed that the occurrence of identity theft and fraud was rife. They further concurred that these crimes are widespread and alluded to them occurring in other cities as well. The participants attested to the fact that the SAPS SCCU is the only Unit within SAPS that investigates cases of identity theft, fraud and corruption that exceed the monetary value of 500 000 in KZN.

6.3.2 The causes of identity theft and fraud in Durban

Questions were directed to address the second objective of the study which sought to investigate the causes of identity theft. The aim of this objective was to determine if SAPS investigating officers from their interaction with such thieves understood the mindset of perpetrators who commit identity theft and fraud, and particularly if they understood their reasons for doing so. The participants concurred that identity theft and fraud perpetrators commonly deliberately committed their crimes in areas where they were unknown. The perpetrator would reside in that area for no longer than three months, commit fraudulent acts, and relocate to the next targeted location. The perspective drawn from the research participants was that of sober and purposive actions by perpetrators. This finding links with the RCT, which proposes that the responsibility for the commission of the crime if ID theft rests with the perpetrator who is completely rational and purposive when this crime is committed, while it is guided by goal oriented decisions. The participants' revealed their understanding of the modus operandi of identity theft and fraud syndicates. They comment in-depth on the techniques they utilise, referring to them as high-frequency and high- technology methods, which is a finding that also supports the principles expounded by the RCT. The participants were in agreement that the main purpose of identity theft and fraud is financial gain. This corroborates what the RCT proposes, which is that criminal events generally occur with the purpose of achieving a certain outcome, be it pleasure, revenge, or financial gain. The participants mentioned that the perpetrators of identity theft and fraud are often highly educated and intelligent, which may explain why so many get away with this crime. This also attests to their level of precision and planning, and particularly points to those who use high-frequency and high-technological methods.

In this exploration of the causes of identity theft and fraud, it was pivotal to gain an understanding of the factors that render victims targets and vulnerable to this crime. This objective thus attempted to unlock the mindset of perpetrators through determining the type of victims' perpetrators target when they commit ID theft and fraud. It is noteworthy that the literature stipulates that identity theft and fraud victims are not limited to a specific gender, race, age, or ethnicity, but that anyone is a potential victim. The participants concurred, and also added a different perspective by referring to companies (thus large entities and not individuals) that fall victim to this crime when their

trademarks or logos are stolen and compromised. Such perpetrators manufacture and sell counterfeit goods and products under the stolen trademark, and these products are commonly known as 'fakes'. Identity theft and fraud victimisation is thus not limited to individuals, but has been broadened in scope as companies and organisations are now also targeted.

6.3.3 Effectiveness of strategies utilised by the SAPS in policing identity theft and fraud

This study was also motivated by the desire to determine what consequences victims suffer following identity theft and fraud. The literature refers to large amounts of money lost due to financial fraud that stains victims' record and reputation. Therefore, the fourth objective of the study sought to examine how the SCCU measured the effectiveness of the strategies that they utilise when dealing with cases of identity theft and fraud. According to the participants, such cases are success driven. Methods of operation seem to be measured by the successful resolution of cases that are received and investigated. These officers are exposed to performance assessments according to which each investigating officer is assessed in regard to the various crime categories the Unit investigates. The number of cases received are compared to the number of cases solved, and this process then assists in determining the effectiveness of the investigative methods employed by each investigating officer. If the number of cases received by investigators is higher than the number of convictions, they are then required to revisit their techniques and methods. The participants stated that most cases of identity theft and fraud that they had investigated had resulted in convictions, which suggests that their investigative strategies and procedures were effective. However, determining this assumption based on actual successful prosecution data was beyond the scope of this study.

To address this gap, the researcher perused various pieces of information in the literatures to compare the participants' responses with the extent of unresolved cases of identity theft and fraud. Based on this review it appeared that some victims had been stuck with the dilemma of ID theft for years without any resolution. There thus seems to be a gap in the numbers and facts that are reported concerning the management and resolution of identity theft and fraud cases. Identity theft and fraud should be frequently and widely addressed on various platforms. Therefore, as other common crimes are widely reported, so should these crimes. Once criminal events of this kind

have been reported to local police stations, investigating officers should see to it that these cases are resolved and, most importantly, that the names of victims are cleared regardless of whether the perpetrator is caught or not. When victims find themselves in the unenviable situation of having had their identity documents stolen and used for fraudulent purposes, the only information they receive is that they are now allegedly married, opened a credit account, purchased goods or used a service, or committed a crime. Issues concerning the investigation to determine how this fraud came about and who was responsible are not victims' responsibility as it is not within their power to acquire the kind of information needed to clear them of any criminal involvement or association with the fraudulent act. There should not be any expectations placed on the victim apart from compliance with the law. Therefore, it is imperative for investigating officers, be it within the SAPS or any other department where such cases are reported, to see to it that the victim does not continue to suffer any more trauma due to the unfortunate commission of the crime to which they fell victim. Any more suffering endured by victims after they have reported these crimes can be seen as secondary victimisation. Relevant departments and institutions can remedy the situation by ensuring that they conduct effective investigations without placing any more responsibility, strain or trauma on victims.

6.3.4 Challenges faced by SAPS SCCU with regards to policing identity theft and fraud

Investigating the policing of identity theft and fraud in Durban requires close examination of any challenges that might impede the effective functioning of the SCCU. The participants offered their honest views on the challenges and difficulties they were subjected to when investigating cases of identity theft and fraud. They referred to limited resources, a heavy workload, a lack of manpower, difficulty in identifying 'invisible' suspects due to the digital nature of these crimes, and noncompliance by affected institutions and departments. Each of these challenges, in their unique way, resulted in the SCCU's inability to function effectively in investigating all identity theft cases and apprehending responsible perpetrators. It is important to note that the participants admitted that, although some of these challenges negatively affected progress and the efficiency of investigations, cases were in many instances resolved with perpetrators apprehended and brought to justice.

Identifying the challenges in curbing the crimes under investigation was crucial in order to understand the issues that need to be addressed and resolved for the smooth functioning of this Unit, and ultimately for the resolution of any cases of identity theft and fraud. As was mentioned, issues such as limited resources, heavy workloads, and low manpower in the SAPS may fortunately be resolved as recent changes were made regarding the staff employment allocations in the SAPS.

An important challenge that was mentioned by the participants was the identification of suspects. This is a particularly difficult process in cases of identity theft and fraud as finding the victim is not as complicated a process, which is in contrast to the identification of a perpetrator who has assumed a victim's identity. Noncompliance by implicated departments and institutions also seems challenging and time consuming to resolve. Some participants mentioned that they were able to get certain information from and the cooperation of these departments using Section 205, but most expressed their concern regarding the lack of assistance from certain departments and institutions. All in all, investigations into cases of identity theft and fraud can be seen as tedious and time consuming, therefore it is imperative to utilise all possible means to assist in the efficient functioning of investigating officers. This can be facilitated by the cooperation of those that the police request assistance from. It is pivotal to clear the victim of complicity and prevent further victimisation of any other person by apprehending and prosecuting those responsible.

6.4 The Way Forward

A criminal activity or trend should be deterred in one way or another if complete eradication proves somewhat difficult. This brings us to the fifth objective of the study, which sought to look at recommendations to curb the scourge of identity theft and fraud in KZN, Durban. Questions were directed at the participants concerning the strategies that they utilised, or that they knew were being utilised, to deter this epidemic. The participants referred to different fraud campaigns that would be launched by the SCCU from time to time, such as conscientising the public of scams that they had been notified of by departments such as the MIC Office and the CIU. The researcher's main concern with the aforementioned strategy is that it put the onus for action to clear their name on victims and the public while investigations are in progress. There should also be strategies to deal

with the *prevention* of such criminal acts on the part of protective services. Such strategies can be designed and facilitated based on valuable research that has been conducted in this field as these projects include information about the different causes of identity theft and fraud as well as the modus operandi of perpetrators. Thus advanced Firewalls and other security measures should be used to ensure that syndicates are unable to identify opportunities to commit these crimes. The researcher understands that the main function of the SAPS is to respond to crime, which means they are called upon to assist after a crime has occurred. Having said this, it is also their responsibility to ensure the safety of all citizens. This means that prevention is also part of their mandate, and thus relevant officials need to study the ever changing modus operandi of perpetrators and the causes of crime in order to combat and prevent escalating crimes such as identity theft and fraud. The implementation of such an approach, together with well-designed and -disseminated awareness campaigns initiated by the SCCU, can result in more effective ways of combating identity theft and fraud.

In any research project where the objectives have been achieved, it is obligatory to offer recommendations based on the findings. This will address future similar challenges and enhance knowledge regarding how to deal with the issues that emerged. The following are the recommendations that are offered in response to the themes that emerged from the data.

6.4.1 Stringent policing of foreign national residency and fraudulent marriages

Many fraudulent marriages result from the challenging socio-economic conditions faced by foreign individuals in their countries of origin. Even though it is saddening that inhumane conditions and difficulties are faced by so many people, fraudulently initiating marriage is not the appropriate response to such challenges. Not only is this illegal, but it has disastrous consequences for the victims of this crime. For instance, victims may thereafter be unable to marry the person of their choice and/or may lose the right to own assets in their own name due to the type of marriage they were fraudulently forced into. Such information may help to create a profile of perpetrators when investigating fraudulent marriage cases. Officials may also be made aware of what types of documents will be submitted to them. In the participants' experience, potential victims are generally Indian women, and they felt that such victims should be cleared of any suspicion that

marriage officials may have when a Pakistani fraudulently married a South African citizen. While some foreign nationals commit fraudulent marriages for the purpose of citizenship and a somewhat better life, others do so with the sole purpose of engaging in the most appalling criminal activities. Investigating and curbing fraudulent marriages is the responsibility of many role-players. The DHA and SAPS have an imperative role to play in monitoring and ensuring that the offence of fraudulent marriages is not successful. Defence and protection should be seen as the main functions of protective services, and they should not merely focus on response to crime.

6.4.2 Visible policing and inspection to combat identity theft to sell counterfeit goods

The issue of counterfeit goods has been explored in many earlier studies, but it was not done so in light of identity theft and fraud. The manufacturing and selling of counterfeit goods was exposed by this study as resulting from the theft of a trademark which is a unique identity that belongs to a company or organisation. The importance of highlighting this type of identity theft is that it has dire economic implications not only for the affected company, but for the country as well as millions of Rand may be lost in revenue and tax income. The production of counterfeit goods does not only have economic implications, but serious negative health impacts as well when counterfeit food, medicine and cosmetic products (including sanitary towels) are manufactured and sold to the general public. In many instances it is difficult to distinguish a counterfeit item from the original product. Education alone is not sufficient to identify such products that are easily accessible and cost effective. Apprehending the guilty syndicates also proves challenging as many individuals purchase these items due to product affordability. Therefore, awareness and education regarding such products are imperative, but a more effective approach will be mandatory visible policing and regular inspections of convenience stores. Inspection is pivotal as it has serious legal implications for perpetrators should they be found guilty of selling counterfeit products. Visible policing and inspection should not only apply to convenience stores, but to all consignments arriving in the country. Consignments should thus be effectively monitored on a permanent basis without waiting for ‘tip offs’ that counterfeit goods are being delivered or shipped into the country. Thus every consignment should be efficiently inspected.

6.4.3 Employment of additional Qualified Staff to ease Workloads and Improve Efficiency

The issues of a lack of manpower and heavy workloads should be addressed due to the concern that they prevent efficient resolution of cases. These challenges cause a backlog in cases that are left unattended, which is not only stressful to employees but more so to the victims of identity theft and fraud. The main goal when an individual is a victim of ID theft is to clear their name of any associated subsequent criminal activity and to continue with their lives as law-abiding citizens. This is particularly important for victims who suffer greatly due to financial losses or a fraudulent marriage. Therefore, lack of resources and manpower should be addressed by the SAPS through the employment and deployment of appropriately trained officials to ensure that all cases are attended to and given the necessary amount of time and attention. As mentioned by a participant, the employment of qualified individuals should be in accordance with the requirements of the work that needs to be done within each unit and department. This will facilitate effective investigations, the ability to apply the cognitive intelligence demanded by such cases, yield positive results leading to convictions, and the clearing of victims who are indeed innocent.

6.4.4 Implementation of the Law that Regulates Compliance by Implicated Organisations and Departments.

Another challenge that was highlighted by the participants is noncompliance by affected departments and organisations, usually to protect their reputation. Businesses fear being associated with any negative actions or criminal activities that may expose them and lead to negative publicity. If this happens, it creates fear and clients lose trust in them and disassociate themselves from these institutions. In an effort to avoid this, an organisation may then opt to resolve the issue internally. In such instances the victim may be found innocent and cleared in order to avoid any negative publicity, but the perpetrator goes unpunished. This opens opportunities for criminals to find their next victim, which possibly causes more harm than was done previously. An organisation's aim when a client has been subjected to a fraudulent act should therefore by not only to protect the image of the organisation, but the well-being of the victim as well. Contrary to organisations' belief, working with the police may not have such negative ramifications; rather, an organisation may be hailed for helping to apprehend the perpetrator and resolve the crime, and

also for assisting in curbing this crime. In turn, this may instil fear among perpetrators who may then avoid any further attempts to defraud that organisation's clients. With this being said, the law should allow investigating officials the right to acquire all the necessary information from an institution in order to eventually apprehend and convict the perpetrator. The participants mentioned that they had been able to acquire phone records using section 205; however, this is often a lengthy procedure to process. Any information requested by police officials regarding an ongoing investigation should not be denied, and neither should it be allowed to drag on for an extensive period of time as this allows the perpetrator time to flee and compromises the way a victim's integrity is viewed. Compliance is thus imperative and should not be made difficult, therefore using the power of the law to assist police officials in this regard is important.

6.4.5 Identification of the suspect

The themes that were discussed above relate to the main premise of the study, which was to investigate the effectiveness of policing identity theft and fraud in Durban by the SCCU. This investigation included any factors that might inhibit effective policing of these types of crime. Difficulties in identifying ID theft perpetrators were highlighted by all the participants. These challenges are due to the 'invisible' nature of perpetrators who are difficult to trace as they have assumed the identity of another, often by untraceable digital means. Not much can be said concerning the identification of such suspects, apart from pointing out that the challenge of non-compliance is an issue that all the investigating officers battled with. This study thus argues that identity theft and fraud cases are complex and require the assistance, compliance and patience of all parties involved in order to successfully identify and apprehend individuals and syndicates who commit this crime.

6.4.6 Usefulness of an Automated Identifying System

Installing an automated identification system in all digital systems seems to be the most preferred protective measure to curb ID theft and fraud. Data that can only be associated with a particular individual are collected fraudulently by means of online facilities (Kodl and Lokay, 2001:2). Thus installing a protective system to counter this is proposed by Roger Clarke in his human

identification theory. According to the participants' responses, such a system is utilised by the DHA and has assisted the SCCU immensely during investigations. This system uses biometrics such persons' signatures, fingerprints and photos to distinguish one individual from the other. It is used as an authenticating system that confirms that individuals are who they say they are. Not only does it involve biometrics, but it also includes knowledge- and token-based authentication. It has thus been less difficult to clear victims in instances where, for example, an ID was stolen and the perpetrator replaced the victim's photo with his own. The DHA is able to examine the photo appearing on the ID and see that it is not the one captured on their system. Therefore, the use of biometrics, knowledge- and token-based authentication is imperative in preventing access to personal accounts and/or social media. It further assists in investigations of identity theft and fraud and can be used to clear the victim and possibly catch the perpetrator. However, some argue that ID theft and fraud still occur regardless of the use of such systems, as crimes are orchestrated by perpetrators who are familiar with the use of high technology. It is thus recommended that such systems be updated on a regular basis to facilitate security checks, to ensure that users' accounts are consistently protected, and that they are confirmed as the original owners of accounts or particular documents. This may prevent identity theft and fraud perpetrators from gaining knowledge regarding how to enter into and take over victims' accounts due to an ever evolving and consistently updated system of digital security.

6.4.7 Measures to Report and Respond to ID Theft and Fraud

Identity theft and fraud are crimes that have serious implications for victims. It is thus important that victims and the general public should be informed about the measures they should follow when they fall victim to these crimes. Institutions such as banks, the DHA, retails stores, and online platforms should advise their clients of any protective measures in place. They should even go as far as creating and installing reporting mechanisms for their clients to enable them to report such cases should they suspect any criminal activity. Identity theft and fraud may not be physically harmful as opposed to other violent crimes, but they are just as impactful. Therefore, a clear understanding of the procedures that need to be followed when victimised should be widely publicised. The SAPS must play its role in ensuring that the general public can rely on them for protection when such crimes have been reported at police stations. The process should not be

terminated after the victim has reported a crime, but the investigation should proceed and, most importantly, the victim must be constantly updated by the investigating officer of information regarding the case. This is to prevent lagging, which can result in the investigation taking longer than it should. No department, organisation or business should turn away a victim without providing information as to how they should go about receiving assistance if they have fallen victim to identity theft and fraud. It is also not acceptable to blame the victim without conducting a thorough investigation. Victims should not go through secondary victimisation in the process of attempting to resolve a case. The presumption and legal principle of 'innocent until proven guilty' must apply to victims of identity theft and fraud.

6.4.8 Using perpetrators' known modus operandi to formulate prevention measures

It may be argued that it is difficult to combat identity theft and fraud when perpetrators' modus operandi constantly change. 'Unconventional methods' are therefore utilised by the SCUU when soliciting information regarding the methods used by perpetrators to commit these crimes. According to the participants, using these methods often takes months before they yield positive results. Thus, in order to be familiar with and stay abreast of perpetrators' modus operandi, knowledge should be obtained about these criminal methods in order for the police to deter these crimes and devise effective preventative measures. In light of this, it is recommended that measures be taken to prevent any perpetrator or syndicate of identity theft from committing the same crime using an identical MO already identified by the police. Every MO that has been utilised should be eradicated by the implementation of a protective measure in response to it. This will make it difficult for any other perpetrator to commit the same crime. Organisations such as SABRIC and SAFP, and all other official data publishing platforms, should gather and publicise such information constantly in order to conscientise every at risk entity. These entities will then be able to establish security and protective measures to combat identified theft risks. The study encourages the protection of victims by means of the most functional and effective techniques to prevent opportunities for perpetrators of crime to commit their devastating deeds.

6.4.9 Response to Curbing Identity Theft and Fraud: Awareness Campaigns and Security Systems as Preventative Measures

When the participants were asked to comment on the methods currently in place to prevent identity theft, they all agreed that awareness campaigns were the most prevalent. Initiating an awareness campaign is useful in reaching out to the masses and cautioning them on matters such as crime. The participants referred to fraud awareness campaign platforms such as radio and television. These platforms reach thousands of people at the same time and can therefore be effective if utilised appropriately. Awareness campaigns are useful in alerting and expanding the general public's knowledge regarding current crime trend, methods and scams. It is thus recommended that such awareness campaigns should cover all geographical areas, even deep rural areas where people are vulnerable. Moreover, the messages should be communicated in all languages and should include persons with disabilities.

A concern regarding the above is that, if the initiation of awareness campaigns is the only strategy to prevent the crimes of ID theft and fraud as proposed by the participants, it will not be enough. This strategy is useful and effective, but it is inadequate in preventing perpetrators from continuing their efforts to defraud unwary citizens. Focus should also be placed on the perpetrators of identity theft and fraud and how they can be inhibited from committing their crimes. In this regard, it is strongly recommended that systems be put in place that will alert not only the victim, but the SAPS, institutions, and businesses should any suspicious activity occur regarding victims' personal information. Many may underplay the responsibility that the SAPS has and must play in protecting South African citizens, yet this organisation is mandated at all times to educate the public to be aware of new crimes. The responsibility of protecting citizens and preventing crime is vested in the SAPS, and communities look up to them to protect them from harm. Protective bodies and online platforms, albeit banks, organisations, institutions or businesses that use payment systems that require personal identifying information, should constantly develop security systems that protect this information. Such systems should be constantly updated by regularly changing codes and any other details that contribute to securing information pertaining to customers, clients and members.

6.4.10 Planning to Deter Identity Theft and Fraud

In order to develop and manage strategies to curb identity theft and fraud, studying and monitoring the prevalence of these crimes should be preceded by a development plan to combat this menace. The respondents were asked to stipulate if identity theft and fraud were seasonal or if they occurred throughout the year, and they agreed that such crimes occurred all year around. They highlighted that such scams and fraudulent activities increased during the Festive Season in December. It thus seems that identity theft and fraud occur everywhere and at no specific point in time, unlike the theft of cars that might be concentrated in areas with large parking lots. Information of this nature should be used to formulate recommendations for the implementation of preventative measures that will curb ID theft throughout the year. This implies that awareness campaigns that expose fraudulent scams and identity theft in particular areas and contexts should be vented from various platforms on a continuous basis. These preventative measures must then be intensified during the Festive Season, as this is when most acts of crime, including identity theft and fraud, generally occur. Focus should not only be on police visibility, but on preventative measures as well. Every store, car dealership, bank, organisation and business that is vulnerable during this time should be sensitised to potential victimisation. Therefore, all entities as well protective bodies are responsible for and should intensify their security systems, particularly in December, as this is when crime peaks.

6.5 Conclusions

Identity theft has been a scourge in the South African society for many years. This crime ranges from the theft of IDs from bags or purses for the purpose of credit card fraud to high technology scams that defraud unwitting victims from thousands of Rand. The Electronics Communications Transmission Act No. 25 of 2002 (Republic of South Africa, 2002) was enacted with the purpose of counteracting cyberattacks, child pornography, and identity theft and fraud. The ECT Act has been used to combat these crimes for more than a decade, and regulates ecommerce in dealing with privacy issues and electronic government services. Due to the inadequacy of the principles that underpinned the premise of this Act, the POPI Act No. 4 of 2013 (Republic of South Africa, 2013) was later established and was signed into law on 26 November 2013. Regardless of the

existence of these Acts, crimes of identity theft and fraud have escalated in conjunction with the emergence of many other types of fraudulent practices every day.

The findings that emerged from the data concur with the literature in many respects, with a few additional factors that may be added to the pool of knowledge regarding identity theft and fraud in the current digital era. For instance, some elements of the modus operandi of ID theft and fraud perpetrators that were mentioned by the participants have not been highlighted in the current literature. Existing literature on data made available by data collecting systems such as SABRIC proved to be updated and on track in light of the various types of identity theft and fraud, even though actual comparative data analyses were beyond the scope of this study. It is noteworthy that these data sites include scholarly articles, but that none offer specificities of the modus operandi of identity theft perpetrators. The current study was able to solicit in-depth information with regards to the MO of perpetrators during the commission of different types of identity theft, such as in incidences of fraudulent marriages, the interception of online transfers and emails, and the production and sale of counterfeit goods. The information that was elicited regarding investigation processes granted the researcher extensive knowledge, such as the fact that section 205(3) of the Criminal Procedure Act (CPA) permits investigating officers to retrieve and examine phone records during an investigation.

The methodology that was utilised by the study was highly appropriate as it allowed the researcher access to information that addressed all the objectives and questions that the study explored. The researcher's use of the qualitative approach resulted in extensive and detailed data. With the use of the NVIVO software, the researcher was able to organise and sort a large bulk of information. By structuring and organising the data, the identification of themes was facilitated. Using thematic analysis, the data were coded and pertinent themes were identified.

The three theories that underpinned the study were the rational choice theory, the routine activity theory, and the human identification theory. The principles of the RCT are congruent with the explanations given by the participants with regards to the mindset of individuals and syndicates who perpetrate identity theft and fraud, as their methods indicate rationality and purposive intent. This may be associated with the level of expertise applied in their crimes. The technological

advancement in their MO is evidence of and consistent with the analogy that much thought and planning are entrenched in the commission of these crimes. This indicates that crimes of identity theft and fraud are facilitated by people of sober mind who have the rational intent of committing a crime for the purpose of financial gain.

The second theory that was applied, namely RAT, explain how perpetrators commit identity theft and fraud. For instance, the participants mentioned the prevalence of identity theft all year round, and that it peaks in December. This is month is known as the Festive Season when people tend to splurge and make large purchases. For this reason, identity theft and fraud syndicates are said to take advantage of people's lack of vigilance to commit their crimes. The RAT principles are consistent with the above factor as, due to the familiar carelessness with money during December, furniture shops, car dealerships, and many other stores and companies are as not as guarded as they normally are during the course of the year. With this lack of guardianship, the presence of suitable targets (i.e., potential victims who carelessly roam the streets during the Festive Season), and likely offenders who are always lurking, waiting for the opportunity to strike, this situation is ideal for the commission of identity theft and fraud. Moreover, hacking and intercepting online money transfers are rife due to a lack of intense and continuously updated security systems, which allows likely offenders to commit identity theft and fraud.

Professor Roger Clarke's human identification theory (HIT) was developed in an effort to support people's need to protect personal identifying information. The researcher used this theory to explain the victimisation of identity theft and fraud victims. HIT stipulates three characteristics that will determine the protection of personal identifying information, namely knowledge-based authentication, token-based authentication, and physical authentication. Any system in place that facilitates any of the above characteristics allows an individual to possess data that will exclusively identify him/her. Should any other person(s) attempt to access this identity, they will need the above authentication data, which is impossible as these data are unique to each individual. Departments such as the DHA utilise this system, for example they use the fingerprints and a photo that are unique to each person. SCCU in this regard has been able to acquire the assistance of DHA during investigations in order to identify a victim and/or perpetrator. Therefore, organisations without such a system place their clients at risk of victimisation. Thus it is imperative that an

authentications system be implemented in order to protect clients against identity theft and fraud, and this is also required for online platforms.

6.6 Concluding Remarks

The approach that this study adopted sought to understand the recent escalation in identity theft and fraud. In this regard, the policing of identity theft and fraud were examined in an effort to unravel and understand these rising figures from the perspective of those responsible for policing and deterring these crimes. In doing so, the study uncovered the realities faced by investigating officers in their line of work. It revealed the different challenges faced by these SCCU officials when investigating crimes of identity theft. The participants' responses extensively considered the various modus operandi utilised by such syndicates, which was identified as a gap in the existing literature as it currently does not expound information of this nature.

The objectives of the study were thoroughly addressed although the researcher was not privy to certain sensitive information that, due to police policy, the participants could not divulge. However, sufficiently rich information was relayed so that the aim and objectives of the study were achieved. A strong emergent element is the danger associated with the crimes of identity theft and fraud in the form of unknown and 'invisible' suspects who hide behind stolen identities and in the maze of digital intricacies. This was identified as a major difficulty concerning the investigation of such crimes. Recommendations were offered to render this less difficult for investigating officers and to allow them to do their work to the best of their ability.

The data suggest that there is evidence of a continuing increase in fraudulent marriages that are perpetrated by foreign nationals. This is a fact that cannot be ignored as it begs the question why illegals who enter the country are allowed to get away with this. Moreover, questions are also raised regarding the lack of measures to monitor the duration of residency by foreign nationals in South Africa, particularly in Durban.

Evolving advancements in the methods utilised by identity theft and fraud perpetrators is also a matter of grave concern. Having entered into the Fourth Industrial Revolution that encourages the

use of online platforms as a means of communication and work, the risks that identity theft and fraud pose should be closely examined. Furthermore, the punishment that is meted out to the perpetrators of such crimes and that used to be deemed sufficient now seem inadequate. Merely confiscating what the perpetrator stole from a victim and even hefty fines are inadequate as these crimes continue to rise.

The researcher lists the following as proposals for future studies within the field of identity theft and fraud:

- Studies should investigate if the punishment meted out to identity theft and fraud perpetrators is sufficient to prevent future offending.
- The dangers of using online platforms in the face of so many advanced techniques available to perpetrators of identity theft and fraud, particularly in the context of the Fourth Industrial Revolution, should be explored.
- Many propose that action should be taken to prevent identity theft and fraud by foreign nationals and that their entering of and residency within the country should be more rigorously controlled. This should be closely monitored and studied by future researchers.

REFERENCES

Abubakar, A., Zadeh, P.B., Janicke, H. and Howley, R. 2016, June. Root cause analysis (RCA) as a preliminary tool into the investigation of identity theft. International conference on cyber security and protection of digital services (Cyber Security), pp. 1-5. IEEE.

Acquisti, A. and Grossklags, J. 2007. What can behavioral economics teach us about privacy? *Digital Privacy: Theory, Technologies and Practices*, *18*.

Ahmed, S.R. 2020. *Preventing identity crime: Identity theft and identity fraud: An identity crime model and legislative analysis with recommendations for preventing identity crime*. Boston: Koninklijke Brill.

Akanle, O. and Shadare, B.R. 2020. Why has it been so difficult to counteract cybercrime in Nigeria? Evidence from an ethnographic study. *International Journal of Cyber Criminology, 14*(1), pp. 29-43.

Alfreds, D. (2015). Here's how easy it is for crooks to steal your ID. *News 24*.

Allison, S.F., Schuck, A.M. and Lersch, K.M. 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, *33*(1).

Anderson, K.B. 2005. Identity theft: Does the risk vary with demographics? *FTC, Bureau of Economics Working Paper*, p. 279

Anderson, K.B. 2006. Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), pp. 160-171.

Anderson, K.B., Durbin, E. and Salinger, M.A. 2008. Identity theft. *Journal of Economic Perspectives*, *22*(2), pp. 171-192.

Artal, R. and Rubenfeld, S., 2017. Ethical issues in research. *Best Practice & Research Clinical Obstetrics & Gynaecology*, *43*, pp.107-114.

Asenahabi, B.M., Busula, A.O. and Ronoh, R., 2019. A choice dilemma in selecting an appropriate Research Design. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 8*(8), pp.348-356.

Austin, J., 2005. Identity and identity formation. In: Culture and identity, 2nd ed. Pearson Education Australia, Frenchs Forest, pp. 7-15.

Bazeley, P. and Jackson, K. (2013). *Qualitative data analysis with NVivo*. London: Sage.

Bellah, J. 2001. Training: Identity theft. *Law and Order*, *49*(10), pp. 222-227.

Black, R.B. 2001. Legislating US data privacy in the context of national identification numbers: Models from South Africa and the United Kingdom. *Cornell Int'l LJ*, *34*, p. 397.

Bose, I. and Leung, A.C.M. 2019. Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, *43*(1).

Botha, J.G., Eloff, M.M. and Swart, I. 2015, August. The effects of the PoPI Act on small and medium enterprises in South Africa. *Information Security for South Africa (ISSA)*, pp. 1-8. IEEE.

Brown., J. 2017. South Africa posts 4.5 billion credit, debit card fraud over 7 years. *City Press.* Available from: http://www.fin24.com/Economy/sa-posts-r45bncredit-debit-card-fraud-over-7-years-20170505 [Accessed: 2017/05/16].

Bryan, L.L. 2020. Effective information security strategies for small business. *International Journal of Cyber Criminology*, *14*(1), pp. 341-360.

Bryman, A. 2015. *Social research methods*. Oxford university press. Available from: https://books.google.co.za/books?hl=en&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&dq=Research+objectives+in+social+science+research&ots=dnRwBYO6rc&sig=AbK2Ovf3VQjUUlZm51PQY-8kjEo#v=onepage&q=Research%20objectives%20in%20social%20science%20research&f=false

Burke, R.H. 2017. *An introduction to criminological theory*. Fifth Edition, Routledge: New York,

Button, M., Lewis, C. and Tapley, J. 2009. *Fraud typologies and the victims of fraud: Literature review*. University of Portsmouth: London.

Cassim, F. 2015. Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal, 18(2).* Available from: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812015000200003

Chamard, S. 2007. Routine activity theory. *The Blackwell Encyclopaedia of Sociology*. Willey: Wiley Online Library.

Clarke, R. 1994. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), pp. 6-37.

Clarke, V. and Braun, V., 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The psychologist*, *26*(2).

Cohen, L.E. and Felson, M. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, pp. 588-608.

Cohen, L.E. and Felson, M. 2010. Social change and crime rate trends: A routine activity approach (1979). *Classics in environmental criminology*, pp. 203-232. Routledge.

Cope, D.G. 2014. Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*(1).

Cornish, D.B. and Clarke, R.V. 2008. The rational choice perspective. *Environmental Criminology and Crime Analysis*, *21*.

Cornish, D.B. and Clarke, R.V. 2016. The rational choice perspective. *Environmental Criminology and Crime Analysis*, in R, Wortley and M, Townsley (eds). Routledge.

Creswell, J.W. and Creswell, J.W. 2007. *Qualitative inquiry and research design: Choosing among five approaches*, 4th edn. Sage: Los Angeles.

Dzomira, S., 2017. Plastic Money and Electronic Banking Services Espousal vis-a-viz Financial Identity Theft Fraud Risk Awareness in a Developing Country. *Journal of Economics and Behavioral Studies*, *9*(5 (J)), pp.255-264.

Eboibi, F.E. and Richards, N.U., 2019. Electronic taxation and cybercrimes in Nigeria, Kenya and South Africa: Lessons from Europe and the United States of America. *Commonwealth Law Bulletin*, *45*(4), pp.716-741.

Eiselen, S. 2014. Fiddling with the ECT Act: Electronic signatures. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *17*(6), pp. 2805-2820.

Farelo, M. and Morris, C. 2006. Status of E-government in South Africa. IST Africa Conference, Pretoria, pp 1-12.

Fokazi, S. 2020. Marriage fraudsters could have their citizenship revoked. *Sunday Times.* https://www.timeslive.co.za/news/south-africa/2020-02-15-marriage-fraudsters-could-have-their-citizenship-revoked/

Gergen, K.J., Josselson, R. and Freeman, M. 2015. The promises of qualitative inquiry. *American Psychologist*, *70*(1), p. 1.

Glaser, D.1971. *Social Deviance*. Chicago: Markham.

Global Economic Crime Survey. 2016. Adjusting the lens on Economic Crime: Preparation brings opportunity back into focus. South Africa: PwC. https://www.pwc.com/gx/en/economic-crime- survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Golladay, K. and Holtfreter, K. 2017. The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), pp. 741-760.

Grant, S. 2006. "I just bought a flat screen TV in Kolkata": Application of laws for international outsourcing related identity theft. *Pitt. J. Tech. L. & Pol'y*, *7*, p. 1.

Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L. and Daly, J. 2007. Generating best evidence from qualitative research: The role of data analysis. *Australian and New Zealand Journal of Public Health*, *31*(6), pp. 545-550.

Harper, D. and Thompson, A.R. eds., 2011. *Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners*. Chichester: John Wiley & Sons, Ltd.

Harrell, E. and Langton, L., 2013. *Victims of identity theft, 2012* (p. 12). US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Hilal, A.H. and Alabri, S.S. 2013. Using for data analysis in qualitative research. *International Interdisciplinary Journal of Education*, *2*(2), pp. 181-186.

Hoar, S.B. 2001. Identity theft: The crime of the new millennium. *Or. L. Rev.*, *80*, p. 1423.

Holt, T.J. and Turner, M.G. 2012. Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, *33*(4), pp. 308-323.

Hoofnagle, C.J. 2007. Identity theft: Making the known unknowns known. *Harv. JL & Tech.*, *21*, p. 97.

Irons, A. and Ophoff, J. 2016. Aspects of digital forensics in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, *11*, pp. 273-283.

Irvin-Erickson, Y. and Ricks, A., 2019. Identity Theft and Fraud Victimization: What We Know About Identity Theft and Fraud Victims From Research-and Practice-Based Evidence. Centre for Victim Research

Jansen, J. and Leukfeldt, R., 2018. Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), pp. 205-228.

Jibril, A.B., Kwarteng, M.A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M. and Chovancova, M. 2020, April. Identity theft on consumer purchase intention: A mediating role of online security and privacy concern. In *Conference on e-Business, e-Services and e-Society*. In: Hattingh M., Matthee M., Smuts H., Pappas I., Dwivedi Y.K., Mäntymäki M. (eds) (pp. 147-158). Springer, Cham.

Joffe, H. and Yardley, L. 2004. Content and thematic analysis. *Research Methods for Clinical and Health Psychology*, *56*.

Joffe, H., 2012. Thematic analysis. *Qualitative research methods in mental health and psychotherapy*, *1*. In: D, Harper and R, Thompson (eds) (pp. 209-223). Chichester: John Wiley & Sons, Ltd.

Jordaan, C. 2008. The Specialised Commercial Crime Unit: An Overview. Available from: https://www.google.com/search?client=firefoxb&noj=1&q=saps+commercial+branch&sa=X&ved=0ahUKEwiE_4H4s_bTAhWlJsAKHfjxDzUQ1QIIbygB&biw=1920&bih=939&gfe_rd=cr&ei=Y_4bWefaBoip8wf90ZYg#

Jordan, G., Leskovar, R. and Marič, M. 2018. Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, *51*(2), pp. 146-155.

Kaefer, F., Roper, J., & Sinha, P. 2015. A software-assisted qualitative content analysis of news articles: Examples and reflections. *Forum: Qualitative Social Research, 16*(2). Hamilton: Institute for Qualitative Research.

Kahn, C.M. and Liñares-Zegarra, J.M. 2016. Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research*, *50*(1), pp. 121-159.

Keenan, J. and Hoshall, D. 2016. Recent IRS activities to combat tax-related identity theft and erroneous refunds. *J. Tax Prac. & Proc.*, *18*, p. 15.

Kempen, A. 2016. Identity fraud-someone: Stole my identity. *Servamus Community-based Safety and Security Magazine*, *109*(12), pp. 36-37.

Kempen, A. 2017. You, your bank cards & card fraud: What are you doing to keep them safe to prevent fraud? *Servamus Community-based Safety and Security Magazine*, *110*(6), pp. 34-35.

Khan, Z.R., Rakhman, S. and Bangera, A., 2017. Who Stole Me? Identity Theft on Social Media in the UAE. *Journal of Management and Marketing Review (JMMR)*, *2*(1), pp.79-86.

Kodl, J. and Lokay, M. 2001. Human identity, human identification and human security. In *Proceedings of the Conference on Security and Protection of Information, Idet Brno, Czech Republic* (pp. 129-138).

Kumar, R. 2014. *Research methodology: A step-by-step guide for beginners*. Thousand Oaks, California: Sage.

Kumaraguru, P., Cranor, L.F. and Newton, E. 2005, September. Privacy perceptions in India and the United States: An interview study. In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)* (pp. 23-25).

Layder, D. 2018. *Investigative research: theory and practice*. California: Sage.

Leukfeldt, E.R., Kleemans, E.R. and Stol, W.P. 2017. A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*(1), pp. 21-37.

Lin, Y.C.J. 2011. *Fake stuff: China and the rise of counterfeit goods*. New York: Routledge.

Luong, H.T., Phan, H.D., Chu, D.V., Nguyen, V.Q., Le, K.T. & Hoang, L.T. 2019. Understanding cybercrimes in Vietnam: From leading-point provisions to legislative system and law enforcement. *International Journal of Cyber Criminology*, *13*(2), pp. 290-308.

Manap, N.A., Rahim, A.A. and Taji, H., 2015. Cyberspace identity theft: An overview. *Mediterranean Journal of Social Sciences*, *6*(4), pp.290-290.

Manning, P.K. 2010. *Democratic policing in a changing world*. New York: Taylor & Francis Group, Boulder. Available from: ProQuest Ebook Central. [Accessed 8 July 2020].

Martina, D. 2017. EU-USA cooperation on information sharing in the fight against terrorism: The roles of privacy and security and the cases of the TFTP and PNR agreements.

Mathews, R.C. 2013. International identity theft: How the Internet revolutionized identity theft and the approaches the world's nations are taking to combat it. *Fla. J. Int'l L.*, *25*, p. 311.

Maxwell, J.A. 2012. *Qualitative research design: An interactive approach* (Vol. 41). California: Sage.

Mayan, M.J. 2016. *Essentials of qualitative inquiry*. New York: Routledge.

McCurdy, M. 2020. *The evolution and legislative response to Nigerian cybercrime.* Doctoral dissertation, Utica College, Nigeria. https://www.news24.com/fin24/economy/sa-posts-r45bncredit-debit-card-fraud-over-7-years-20170505

McNabb, D.E. 2015. *Research methods for political science: Quantitative and qualitative methods*. New York: Routledge.

Miró, F. 2014. Routine activity theory. *The Encyclopedia of Theoretical Criminology*, pp. 1-7.

Monahan, T. 2009. Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, *13*(2), pp. 155-176.

Morse, J.M. 2015. Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), pp. 1212-1222.

Naidoo, S. 2019. South Africa lost R277m to fake goods, says police minister. *Cape Argus.* https://www.iol.co.za/weekend-argus/news/sa-lost-r277m-to-fake-goods-says-police-minister-35965493

Neuman, L.W. 2014. *Social research methods: Qualitative and quantitative approaches*. Boston: Publishers' Design and Production Services.

Newman, G.R. and McNally, M.M. 2005. Identity theft literature review. Washington D.C: National Criminal Justice Reference Service.

Ngema, T. 2017. Card fraud costs South Africa over 600 million a year. *Daily News*. Available from: http://www.iol.co.za/dailynews/news/south-africa/card-fraud-costs-sa-over-r600m-a-year-9165922

Ngidi, T.L., 2013. *Impact of Batho Pele principles on service delivery: A case study of the Durban regional office of the Department of Home Affairs* (Doctoral dissertation).

Ngwenya, J.S. 2015. Crime and courts: Identity thieves becoming more resourceful. http://www.iol.co.za/news/crime-courts/identity-thieves-becoming-more-resourceful-1882461

Nzeakor, O.F., Nwokeoma, B.N. and Ezeh, P. 2020. Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. *International Journal of Cyber Criminology*, *14*(1), pp. 283-299.

Ogunleye, Y.O., Ojedokun, U.A. and Aderinto, A.A. 2019. Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2), pp. 309-325.

Oxford South African Pocket Dictionary, 2015. 4th edn, Cape Town: Oxford University Press.

Parker, C., Scott, S. and Geddes, A., 2019. Snowball sampling. *SAGE research methods foundations*, doi: http://dx.doi.org/10.4135

Pradier, A., Rubin, M. and van der Merwe, H., 2018. Between transitional justice and politics: Reparations in South Africa. *South African Journal of International Affairs*, *25*(3), pp.301-321.

Pratt, T.C., Holtfreter, K. and Reisig, M.D. 2010. Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), pp. 267-296.

Punch, K.F. 2013. *Introduction to social research: Quantitative and qualitative approaches*. London: Sage.

Rahi, S., 2017. Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), pp.1-5.

Republic of South Africa (RSA). 2002a. Electronic Communications and Transactions Act 25 of 2002.

Republic of South Africa (RSA). 2009. Protection of Personal Information (POPI) Bill 9 of 2009.

Reichel, P. and Albanese, J. (Eds.). 2013. *Handbook of transnational crime and justice*. California: Sage.

Romanosky, S., Telang, R. and Acquisti, A. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), pp. 256-286.

Rosenthal, M. 2016. Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning*, *8*(4), pp. 509-516.

Rotenberg, M. 2001. Privacy and secrecy after September 11. (Foreword). *Minn. L. Rev.*, *86*, p. 1115.

Saunders, K.M. and Zucker, B. 1999. Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology, 13*(2), pp. 183-192.

Schwartz, G.J. 2016. *Workplace learning in the South African Police Service (SAPS): Themes and perspectives in teaching research methodology module.* Doctoral dissertation, SAPS national instruction, University of South Africa, Pretoria.

Service. Unpublished document. Pretoria: SAPS.

Shadden, B. 2005. Aphasia as identity theft: Theory and practice. *Aphasiology*, *19*(3-5), pp. 211-223.

Shan-A-Khuda, M. & Schreuders, Z.C. 2019. Understanding cybercrime victimisation: Modelling the local area variations in routinely collected cybercrime police data using latent class analysis. *International Journal of Cyber Criminology,13*(2), pp. 493-510.

Sharma, G., 2017. Pros and cons of different sampling techniques. *International journal of applied research*, *3*(7), pp.749-752.

Shenton, A.K. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), pp. 63-75.

Sherman, L.W., Gartin, P.R. and Buerger, M.E. 1989. Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology*, *27*(1), pp. 27-56.

Sihlangu, J. 2019. Identity fraud and theft on the rise in South Africa compared to 2018. Identity theft is a serious concern for South African citizens. Available from: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

South African Banking Risk and Information Centre. 2019. Available from: https://www.sabric.co.za/

South African History Online. 2011. Port Natal is renamed Durban in honour of Sir Benjamin D'Urban of the Cape Colony 1834-37. Available from: http://www.sahistory.org.za/dated-event/port-natal-renamed-durban-honour-sir-benjamin-durban-governor-cape-colony-1834-37

South African Police Service. 2006. National Instruction 1/2006: Research in the

South African Police Services Annual Crime Report, 2018/2019. Addendum to the SAPS Annual Crime Report. Pretoria: Crime Registrar.

Sproule, S. and Archer, N. 2007, July. Defining identity theft. In *Eighth World Congress on the Management of eBusiness (WCMeB 2007)* (pp. 20-20). IEEE.

Stevens, G.M. 2003. *Privacy: Total information awareness programs and related information access, collection, and protection laws* (No. CRS-RL31730). Washington DC: Federation of American Scientists.

Strauss, A. & Corbin, J. 1990. *Basics of qualitative research* (Vol. 15). Newbury Park, CA: Sage.

Swart, I., Irwin, B. and Grobler, M. 2014, September. On the viability of pro-active automated PII breach detection: A South African case study. In *Proceedings of the Southern African*

Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology (p. 251). ACM.

Taylor, S.J., Bogdan, R. and DeVault, M. 2015. *Introduction to qualitative research methods: A guidebook and resource*. Hoboken, New Jersey: John Wiley & Sons.

Dimitrios, T., Antigoni, F. and Kotrotsiou, S., 2018. Ethics and deontology in nursing research: A discussion paper. *International Journal of Caring Sciences*, *11*(3), pp.1982-1989.

Thukwana, N. 2019. Crime Stats: Sharp rise seen in commercial crimes. *Sunday Times.* https://www.thesouthafrican.com/news/finance/increase-identity-fraud-and-theft-in-south-africa/

Tongco, M.D.C. 2007. Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, *5*, pp. 147-158.

Trochim, W.M. 2007. Research Methods Knowledge Base. Cornwell University. Last Revised: 10/20/200. Available from: https://www.socialresearchmethods.net/kb/

United States. General Accounting Office. 2002, June. Identity fraud: Greater awareness and use of existing data needed. *Publication No. USGAO-02-766*. Washington, DC: US Government.

Unofficial translation, Ministry of Justice. 2015. Finland. https://www.finlex.fi/en/laki/kaannokset/2015/en20150011_20151596.pdf

Van der Meulen, N. 2006. The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union. *Report Commissioned by the National Infrastructure Cyber Crime program (NICC).*

Van Niekerk, B. 2017. An analysis of cyber incidents in South Africa. *African Journal of Information and Communication*, *20*, pp. 113-132.

Varma, T.N. and Khan, D.A. 2017. Curbing cyber-crimes by Indian law. Jamshedpur: Available at SSRN 2922365.

Vieraitis, L.M., Copes, H., Powell, Z.A. and Pike, A. 2015. A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior*, *20*, pp. 10-18.

Villar-Rodríguez, E., Del Ser, J., Torre-Bastida, A.I., Bilbao, M.N. and Salcedo-Sanz, S. 2016. A novel machine learning approach to the detection of identity theft in social networks based on emulated attack instances and support vector machines. *Concurrency and Computation: Practice and Experience*, *28*(4), pp. 1385-1395.

Wahyuni, D. 2012. The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), pp. 69-80.

Wall, D.S. 2013. Policing identity crimes. *Policing and Society*, *23*(4), pp. 437-460.

Wang, W., Zhang, J., Li, Q., Zong, C. and Li, Z. 2019. Are you for real? Detecting identity fraud via dialogue interactions. *arXiv preprint arXiv:1908.06820*.

Wangen, G., Hallstensen, C. and Snekkenes, E., 2018. A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *17*(6), pp.681-699.

Weisburd, D., Waring, E. and Chayet, E.F. 2001. *White-collar crime and criminal careers*. Cambridge: Cambridge University Press.

White, M.D. and Fisher, C., 2008. Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review*, *19*(1), pp.3-24.

Zaeem, R.N., Manoharan, M., Yang, Y. and Barber, K.S. 2017. Modelling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security*, *65*, pp. 50-63.

Zharova, A. 2019. Ensuring the information security of information communication technology users in Russia. *International Journal of Cyber Criminology*, *13*(2), pp. 255-269.

APPENDIX: A

CONFIRMATION OF INFORMED CONSENT

NB: The interview is not a test, therefor there is no right or incorrect answer.

Topic: THE POLICING OF IDENTITY THEFT IN DURBAN.

An Investigation into the policing of Identity Theft: A case of South African Police Service Serious Commercial Crime Unit, Durban, KwaZulu-Natal, South Africa.

Researcher: Ms F.L Kheswa	Supervisor: Dr Londeka Ngubane.
Contact details: lindokheswa07@gmail.com	NgubaneLP@ukzn.ac.za
0789417260 / 0319094624	031 260 2060
University of KwaZulu-Natal	University of KwaZulu-Natal
School of Applied Human Science Department of Criminology and Forensic Studies	School of Applied Human Science Department of Criminology and Forensic Studies
Qualifications: Bachelor of Social Science Honours (Criminology); Bachelor of Social Science (Criminology and Psychology)	Masters of Social Science (Criminology); Bachelor of Social Science Honours Bachelor of Social Science

OR

HSSREC Research Office, Westville Campus, Govan Mbeki Building
Tel: 0312604557/3587
Email: XIMBAP@ukzn.ac.za

Dear esteemed participant.

I, Fudumezile Kheswa a Masters student at the University of KwaZulu-Natal hereby request your full participation in this study which seeks to investigate the policing of identity theft by South African Police Service Serious Commercial Crime Unit (SAPS SCCU).

Description of Project

Objectives

- To assess the nature of identity theft in Durban.
- To examine the effectiveness of the strategies employed by SAPS CCU in policing identity theft in Durban.
- To identify the challenges of policing identity theft in Durban.
- To recommend strategies to curb identity theft in Durban.

The study seeks to explore the strategies utilized by SAPS SCCU in detecting combating and preventing the phenomena of identity theft particularly in Durban. Questions regarding the nature of identity theft, techniques facilitated by the unit as well as areas which are most likely to be subject to identity theft. Main focus being on the progress of policing this crime as well as improvements in techniques facilitated.

Procedure

The researcher will make arrangements with each participant in accordance to one's availability. The interview will be conducted at the participants' choice of location, preferably where there is little or no disturbance. The duration of each interview will approximately take 30 minutes.

Probable benefits

The study will contribute towards information on scholarly journals. Further make many civilians aware of this phenomena as well as ways in which they can caution themselves against this crime. Importantly for SAPS SCCU, guide them towards improved risk assessment strategies to better investigate and or the fight against identity theft. Also assist in designing programs or better ways to deal with victims of identity theft.

Anonymity and Confidentiality

Anonymity and confidentiality is ensured as real names of participants will not be stipulated in the thesis and on the publication of the research. Participants will be fully protected from any harm as the questions pertaining to the research are not personal, the time frame is short /minimal ensuring no physical distress or exhaustion to the participant. The participant may withdraw from the study should they experience discomfort in the questions asked. All participants will be debriefed to ensure that participants feel no harm or anxiety from the study.

As a participant you are well within your rights not to have your interview recorded. Please indicate in the form of a tick if you are willing or not willing to have the interview recorded.

	Willing	Not Willing
Audio equipment		

Your full participation in the study will be of great assistance to the completion of the study.

Participant declaration

I ……. Understand the basis of the topic understudy, and am voluntary willing to participate in the study. I have a full understanding that there is no right or wrong answer. I have the right not to have my interview recorded. I am aware of my right to voice any discomfort in the questions asked moreover the notion to disengage should I feel I can no longer continue.

Name of Participant: Signature:

…….. ……

Date:

……..

APPENDIX: B

THE POLICING OF IDENTITY THEFT IN DURBAN

Interview schedule questions:

Offender based questions

- Are there cases of identity theft Durban?
- Would you say there a lot of such cases?
- What is the most common form of identity theft and identity fraud?
- What would you say is the cause of identity theft in Durban?
- What is the current known modus operandi for identity theft perpetrators?

Victim based questions

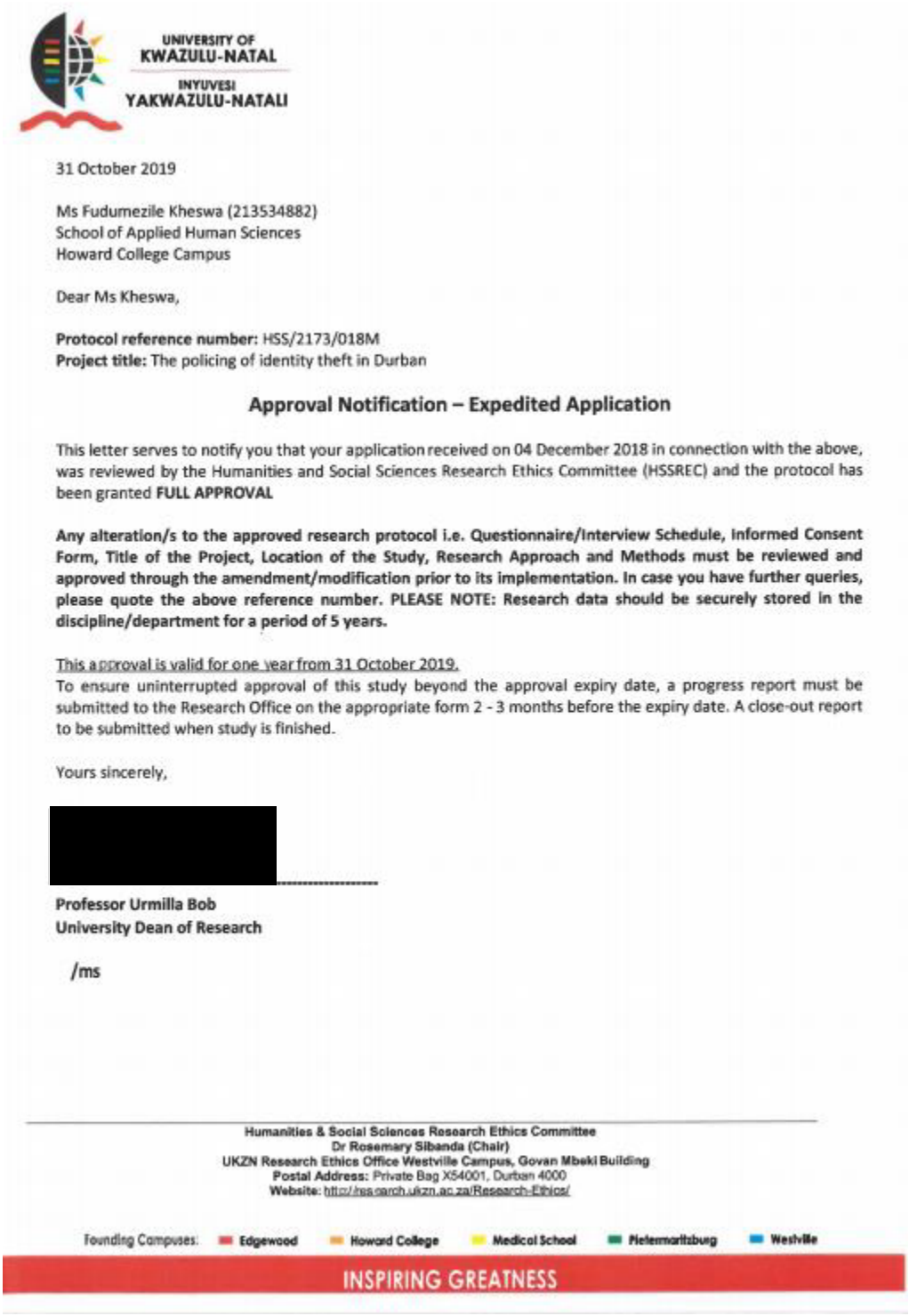
- With whom is the victim in first contact with when requesting to lay a complaint?
- What mechanisms are in place to report identity fraud and identity theft?
- How do these mechanisms operate and or function?
- How do these mechanisms work to assist victims?
- What makes victims most vulnerable to identity thieves?

Policing based questions

- What methodology is currently in place to prevent identity theft from occurring?
- What challenges is the department and or unit faced with in policing identity theft and fraud?

- What strategy is utilised to determine the effectiveness of strategies used to detect identity theft syndicates?
- What is the departments' strategy for identifying current and emerging risks?
- Using the current risk assessment strategies what discoveries were made?
- What measures have been taken by the department and or unit to manage these risks?
- Would you say that identity theft is Seasonal? If yes, when is it most common?

APPENDIX: C



UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

31 October 2019

Ms Fudumezile Kheswa (213534882)
School of Applied Human Sciences
Howard College Campus

Dear Ms Kheswa,

Protocol reference number: HSS/2173/018M
Project title: The policing of identity theft in Durban

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 04 December 2018 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid for one year from 31 October 2019.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

Yours sincerely,

[redacted]

Professor Urmilla Bob
University Dean of Research

/ms

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
UKZN Research Ethics Office Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Website: http://research.ukzn.ac.za/Research-Ethics/

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville

INSPIRING GREATNESS

APPENDIX: D

South African Police Service | Suid-Afrikaanse Polisiediens

Privaatsak / Private Bag X94 | Pretoria / 0001 | Faks nr. / Fax No. (012) 334 3519

Your reference/U verwysing:

My reference/My verwysing: **3/34/2**

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: **Lt Col Joubert**
AC Thenga
Tel: **(012) 393 3118**
Email: **JoubertG@saps.gov.za**

Ms FL Kheswa
UNIVERSITY OF KWAZULU-NATAL

RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: AN INVESTIGATION INTO THE POLICING OF IDENTITY THEFT; A CASE OF DURBAN SOUTH AFRICAN POLICE SERVICE (SAPS) SPECIALISED COMMERCIAL CRIME UNIT (SCCU), DURBAN, KWAZULU-NATAL, SOUTH AFRICA: UNIVERSITY OF KWAZULU-NATAL: MASTERS DEGREE: RESEARCHER: FL KHESWA

The above subject matter refers.

You are hereby granted approval for your research study on the above mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office:

The Provincial Commissioner: KwaZulu-Natal:

- **Contact Person:** Brigadier MM Buthelezi
- **Contact Details:** (031) 325 4946/ 4925
- **Email Address:** ButheleziPN@saps.gov.za

The Provincial Commissioner: KwaZulu-Natal has stressed that participation in interviews will be on a voluntary basis and respondents may refuse to answer questions implying sensitive information.

Kindly adhere to paragraph 6 of our attached letter signed on the **2019-07-18** with the same above reference number.

[redacted]

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

DATE: 2019 -08- 26

1

Turnitin Originality Report

Processed on: 01-Jul-2021 12:12 PM CAT
ID: 1614516507
Word Count: 50698
Submitted: 1

Masters Dissertation By Fudumezile Kheswa

Similarity Index	Similarity by Source	
7%	Internet Sources:	6%
	Publications:	4%
	Student Papers:	2%

include quoted | include bibliography | exclude small matches | mode: quickview (classic) report | Change mode | print | download

<1% match (Internet from 20-Nov-2020)
https://epdf.pub/identity-theft-a-reference-handbook-contemporary-world-issues.html

<1% match (Internet from 24-Nov-2020)
https://epdf.pub/innovating-government-normative-policy-and-technological-dimensions-of-modern-go.html

<1% match ()
Dekeza-Tsomo, Ntombikazi Gloria. "Factors contributing to the dropout rate of learners at selected high schools in Kings William's Town", Faculty of Arts, 2012

<1% match ()
Bestman, Amy. "Pathways to electronic gambling machine venues in New South Wales", Deakin University, Faculty of Health, School of Health and Social Development, 2019

<1% match ()
Naukushu, Shiwana Teeleni. "A critical theory enquiry in the development of number sense in Namibian first year pre-service secondary mathematics teachers", Stellenbosch : Stellenbosch University, 2016

<1% match ()
Villar-Rodriguez, Esther. "Advanced Machine Learning Techniques and Meta-Heuristic Optimization for the Detection of Masquerading Attacks in Social Networks",

Masters Dissertation

ORIGINALITY REPORT

7%	6%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	epdf.pub Internet Source	<1%
2	hdl.handle.net Internet Source	<1%
3	repository.up.ac.za Internet Source	<1%
4	core.ac.uk Internet Source	<1%
5	pdfs.semanticscholar.org Internet Source	<1%
6	www.news24.com Internet Source	<1%
7	www.scielo.org.za Internet Source	<1%