Exploring the Challenges of Forensic Technology in Responding to Identity Document Theft in Polokwane Policing Area, South Africa

William Moyahabo Rakololo[1], Witness Maluleke[2,*] and Jaco Barkhuizen[2]

[1]*Forensic Investigator at Department of Rural Development and Land Reform, South Africa*

[2]*Department of Criminology and Criminal Justice, University of Limpopo, South Africa*

Abstract: This study explores the challenges of forensic technology in responding to Identity Document (ID) theft as an approach used by the South African Police Service (SAPS) in the Polokwane policing area. This study further evaluates the availability of technological and conventional resources to respond to this scourge, as well as the capabilities of the SAPS to utilise the available [lack of forensic technology] resources to respond best to ID theft. This was done by analysing preventative measures, associated with these challenges, as faced by SAPS and other relevant stakeholders on responding to this crime in the Polokwane Central Business District (CBD), Bendor Park, and Flora Park, coupled with the number of stores situated in the business sectors of these selected areas. For this study, the researchers adopted a quantitative research approach with 90 respondents in the identified areas. This study established that the secretive nature of ID theft makes it difficult for the relevant stakeholders (Not limited to the local SAPS, Businesses, and Public members as presented by this study) to effectively respond to this scourge. Negatively, the forefront gatekeepers to respond to this crime are mainly SAPS Constables with less training to investigates ID theft properly. Thus, find themselves being more reactive than proactive, which contributes to the difficulty of locating potential perpetrators in the process of conventional investigations applications. Furthermore, ID thieves utilise advanced technological resources (I.e. Computer hacking software), as opposed to SAPS which does not have systems nor capacity to effectively respond to this crime. The limited resources at the disposal of SAPS also renders its effort in responding to this crime inadequate. For recommendations; significant emphases should be directed on the promotion of public awareness through public education for the use of forensic technology as an investigative and identification tool of responding to ID theft. The intensive training of SAPS officials and inter-governmental corroboration between SAPS, Department of Home Affairs (DHA), and other relevant stakeholders in understanding this technology are highly advised.

Keywords: Challenges, Forensic technology, Identity Document theft, Preventative measures, South African Police Service, South Africa, Victims.

INTRODUCTION

Exploring the challenges of forensic technology in responding to ID theft in Polokwane policing area of South Africa seems to be underutilised. The local SAPS reveals that 'forensic science' is the application of scientific methods in the investigation of crime and specifically the examination of physical exhibit material. The word *'forensic'* is derived from the Latin word 'Forum' and is understood to mean 'for the courts'. The basis of most facets of this field is the Locard Principle. This means that every contact leaves a trace, South African Police Service [SAPS] (2014). The Forensic Science Laboratory (FSL) of the SAPS was formed on 15 January 1971 with the Biology, Chemistry, and Electronics Units. A new building complex was occupied in March 1987 when the Ballistic and *Question Document Unit*, which before this had resorted under the SA Criminal Bureau, was amalgamated with the FSL. Early in 2000, a decision was made to amalgamate the Explosive Investigation Service with the FSL, which was realised on 2000-04-01. In addition to the main laboratory in Pretoria, decentralised offices are established in Cape Town [Western Cape - WC], Port Elizabeth [Eastern Cape - EC], and Durban [KwaZulu-Natal - KZN]. The laboratories in Pretoria [Gauteng - GP] and the WC consist of all the units, while the EC Laboratory has Ballistic and Chemistry Units, and the laboratory in KZN consists of a Ballistic Unit.

The activities of the FSL are the application of scientific principles, methods, and techniques to the process of investigation. In an objective search for the truth, the intention is not only to bring offenders of the law to justice but also to protect innocent people against prosecution. This service includes scenes of crime and the analysis of physical evidence to arrive at a meaningful conclusion (SAPS, 2014).

The SAPS has established various strategies in responding to crime in general. According to the SAPS strategic plan report, the expectation that the SAPS eradicates crime in South Africa without such active involvement is unrealistic. Several platforms exist for such community involvement, the majority of which have been initiated by the SAPS, including the following Community Police Forums (CPF), Crime

*Address correspondence to this author at the Department of Criminology and Criminal Justice, University of Limpopo, South Africa; Tel: 015 268 4881; E-mail: witness.maluleke@ul.ac.za

Stoppers reporting line; recently established Crime Line, Police Reservists; and various community-based crime prevention initiatives such as the Youth Crime Prevention Capacity-building Programmes [YCPCP] (SAPS, 2010).

The current methods used to respond to ID theft are incapable of achieving any real success because they focus on punishment. Currently, financial institutions are only liable to their customer-victims in limited circumstances and offenders regularly escape justice. As a result, monetary penalties and threats of imprisonment have done little to curb the monumental increase in identity thefts over the last decade. This note argues in favour of shifting the policy of dealing with identity theft from punishment to deterrence, and shifting the burden of its prevention from financial institutions to Points-of-Sale (POS) at retail, online, and commercial establishments, Heller (2008). Taking these methods and techniques into consideration, it is clear that the community is engaged in the fight against crime. However, the challenge as perceived by the researchers is that, although they may be involved, the very same public is assumed not to even understand and know the crime of ID theft. Being that as it may, it then becomes impossible to respond to ID theft given the fact that the crime is unknown to them. Therefore, SAPS needs to educate communities of all kinds of profiled crimes so that they know when and how to respond to such crimes.

IDENTITY THEFT: FORENSIC TECHNOLOGY MEASURES

The South African DHA is in the process of implementing the Home Affairs National Identification System (HANIS). This system aims to replace the current paper system with a digital database. HANIS holds the ID numbers, fingerprints, and photos of South African citizens. HANIS can only work as well as those feeding information into it. If the levels of corruption are high within the DHA, then false information can easily be fed into the system (Smith, 2013). Interestingly, a partnership has been concluded between the South African Banking Risk Information Centre (SABRIC) and the DHA in terms of which the banks will be granted real-time access to HANIS for the verification of the ID of prospective and current clients (Smith, 2013). This project is being implemented in phases, with the first phase completed in 2009. The first phase proved the feasibility of online fingerprint verification. The second phase determines the prerequisites for implementing the system and the third phase estimates the costs involved for various stakeholders. A possible fourth phase addressing Information Technology (IT) related issues is expected. It is hoped that this system will make it difficult for people with fraudulent identification documents to use them (Smith, 2013).

The Use of Forensic Technology in Minimising Identity Document Theft Risks

The functions of the SAPS FSL Questioned Document Unit are based on the rendering of an effective Question Document examination service. The examinations conducted by this Unit are demarcated to the following:

- **Handwriting individualisation:** By comparing the individual writing characteristics present in the writing on a disputed document with those in the specimen writing of a specific person, it can be determined whether that person is the author of the disputed document. In such a case, there is an unambiguous connection between the person and the disputed writings as follows:

- **Typewriting:** A typewritten or printed document can be individualised as the product of a specific machine.

- **Erasures, obliterations, additions, insertions, and overwriting on documents** can be detected and, in most cases, the original writing is restored.

- **Forged signatures:** Simulating and tracing of signatures can be determined.

- **Base material (paper):** The material used as a base for the composition of a document can be examined to reveal whether the base material is of a definite type, manufacture, or kind that may be indicative of its origin.

- **Ink and other mediums used on documents:** The use of various inks or mediums on one or different documents can be distinguished. Thus, it can be determined whether additions or changes were made by using another ink or medium (SAPS, 2014).

- **Other apparatus and equipment.** The examination of items such as rubber or metal stamps, printing presses, sealing-wax apparatus, punch-card machines, photocopies, mechanical calculators can be of assistance to investigating officers to determine whether documents were prepared by the same type of machine or, more importantly, to be able to identify a specific machine indentation. Through the application of various techniques (electrostatic detection oblique lighting), indentations on documents originating from previous documents can be made legible.

- **Damaged documents**. Documents that are damaged by being scorched, burnt, soiled, or torn can partially or completely be restored. Counterfeit banknotes. South African, United States of America (USA) dollar and other foreign banknotes are examined with a view of establishing authenticity. Printers' plates and colour laser copies possibly used in the manufacture of banknotes, can also be examined and linked to specific counterfeit notes.

When someone who can describe his relation with computers and the internet as professional or even as an advanced user, reaches to the point that feels insecure and suspicious with the interaction with them, then it appears that the situation requires some attention. The statistics prove that ID theft is a type of old-fashioned crime that transformed into a cybercrime because of the intense ‘investment’ of online sources. There may be more ‘bad’ people in the world than good ones and the spur of committing the perfect crime that will never be revealed still runs in some people's minds. This situation leads to the improvement of tools and the popularity of studying and research in computer forensics in the last few years. It is the type of science that corresponds to the needs of digital investigations. Therefore, for the conditions where ID theft is combined with computer usage, computer forensics is the type of science that will be requested to provide the evidence. In such a perspective, there should be an effort to provide the computer forensic analysts with more detailed and concrete procedures that will help them accomplish their target. For this reason, with respect and based on the computer forensics frameworks aiming to aid digital investigations, there is an approach of investigating ID theft incidents with an independent investigation methodology. The ID theft investigation framework distinguishes the examination in the victim’s and the fraudster's side and the first level of this investigation process analysis were hence presented. This type of investigation method aims to provide results on a more focused basis regarding an ID theft incident. Future work includes a more detailed approach to the findings of the investigation process based on the evidence left behind on a fraudster's digital storage media and the victims accordingly. An experimental assessment on fictional cases by analysing reliable, residual data from hard disk drives will validate the research; and that will be accomplished in two parts, where the researcher behaves as the perpetrator in a closed network attack in the laboratory, and where the researcher uses the evidence that is left behind (from the first experiment) and acts as a forensic examiner, analysing the hypothetical victims’ hard disk drives, Angelopoulou (2007).

The situational prevention divides up the possible techniques into five categories: these include the increase the effort the offender must make to complete the crime; increasing the risks of getting caught; reduce the rewards that result from the crime; reducing provocations that may encourage or otherwise tempt offenders; and removing excuses that offenders may use to justify their crimes in an attempt to prevent ID theft, people need to be knowledgeable of the kind of crime they may be exposed to in the event they lose their IDs, Newman and McNally (2005). The existing popular belief is that prevention is better than cure. People should endeavour not to avail of any opportunities to ID thieves to have access to their IDs. However, this can be done only if the public is aware that all documents entailing their ID number or any other identifying number, may lead them into being victims of ID theft.

Some of the most effective proactive ways for a consumer to minimise their risk to ID theft includes the following as (Albrecht, Albrecht, and Tzafrir, 2011) affirms:

- **Guard mail from theft:** When away from home, have the postal service hold your mail.

- **Guard social security cards and numbers:** An individual’s Social Security (SS) number is valuable information for any ID theft perpetrator. With knowledge of someone’s Social Security number, perpetrators can open all kinds of new accounts in the victim’s name. Therefore, consumers should always keep their SS card in a safe place.

- **Safeguard all personal information:** Safeguarding personal information is very important for every individual. Consumers, who have roommates, employ outside help to clean or perform other domestic services, or have outside people in their house for any reason need to be particularly careful by adhering to the following guidelines:

- **Guard trash against theft:** Consumers need to tear or shred receipts, insurance information, credit applications, doctor's bills, checks and bank statements, old credit cards, and any credit offers they receive in the mail, as well as any other source of personal information. Buying a shredder is one of the wisest purchases individuals can make.

- **Protect the wallet and other valuables:** Consumers should carry their wallets in their front pocket and never leave it in their car or any other place where it can be stolen. It is important for consumers to always be aware of where their wallet is and what its contents are. Individuals should only carry identification information and credit and debit cards that they regularly use in their wallets.

- **Protecting the home:** Consumers should protect their houses from perpetrators. Some perpetrators have been known to break into a home and not steal a single physical object. The victims may not even know someone has been inside their home. The perpetrator will steal all information that is needed to easily commit identity theft and then leave. To prevent this from happening, it is important to lock all doors, preferably with deadbolts or double locks, and lock all windows. It is a good idea to have an alarm system.

It should be [highly] noted that a surprising amount of information may be gleaned from forensic examination of recovered electronic devices. This comes about when seizing computers, cellular telephones, and similar devices. For years, forensic experts have examined these, and valuable evidence has been recovered. However, what is not generally known, however, is that seized Automated Teller Machines (ATM) skimmers, modified POS terminals, hidden cameras, and similar devices may also yield valuable forensic clues for investigators if the technical details of their construction are properly evaluated. On contrary, the 'traditional' forensics such as fingerprints and Deoxyribonucleic Acid (DNA) that can be recovered from such devices, the actual construction of the units or the modifications themselves may yield a surprisingly large amount of useful information for investigators. This evidence or knowledge might lead investigators to a successful conclusion of the case. Some examples follow as discussed by the International Association of Chiefs of Police [IACP] ([sa]):

- Circuit boards that hold the electronic components for "skimming" devices (the material on which parasitic microprocessors and other parts are mounted) often have a fabricator's name or logo silkscreened onto the board. Criminals who mass-produce these boards will often go to a commercial circuit board fabricator for this work. Commonly, the fabricator will include its logo, company name, and most importantly a "run number" or "order number" on the board. This can lead investigators to suspects.

- All integrated circuits and microprocessors as well as some other components have manufacturing codes printed on them. An electronics professional will be able to interpret these codes to determine the date and location of manufacture for the part. From these codes, it may be possible to determine where the part was sold using a list of suppliers. These can help investigators locate the specific supplier of the part, again leading to suspects, as some of the parts used in skimming and overlay devices are not very common.

- To the trained electronics professional, the way the circuit is physically laid out on the circuit board, and the method that the circuit uses to "solve" the problem of intercepting victims' keypad codes, for example, is highly indicative of the demographics of the suspects. Experienced engineers will be able to examine the seized skimming device, look at the parasitic circuit boards and components, and determine the level of the suspects' education, their background in general, and clues to where they obtained that education.

- Electronic and computer professionals can assist investigators in another way as well. Skimming devices are constructed around microcontrollers, miniature computers on a chip. Computers need software (in this case called "firmware") to run. The firmware stored within these systems serves to do the work of intercepting and storing customer data for later retrieval by the suspects. This firmware may be retrieved from the device by electronics and computer system professionals and examined for clues as to its originators. As with the physical hardware, the style and efficiency of the firmware can tell investigators a lot about the suspects.

It should be stated that all the suggested strategies sound very technical. However, the 'Agency leaders' may wonder how they can convince investigators to consider these factors when they seize a skimming device or ATM overlay. Indeed, the examination of seized POS and overlay devices at this technical level is beyond the skill level of most police officers. This is a fact, but it can be addressed most effectively through collaboration with the high-tech industry, IACP ([sa]).

FORENSIC INVESTIGATIONS ON ONLINE IDENTITY DOCUMENT THEFT

Identity theft in its online form is considered a relatively new method of fraud and there is not enough guidance for forensic investigators. The investigator will have to unfold the digital trail of evidence and try to present potential explanations of how such a crime occurred. This digital trail involves examining how a crime was committed using computers and the internet. The investigation should identify how the leak of personal information occurred that made it possible to conduct a misuse of resources such as a credit card number. It should also include details of the misuse such as dates, goods purchased, and amounts spent. If it is possible, the perpetrator should also be identified. The latter is perhaps one of the most challenging tasks as, unlike DNA evidence, computer records can identify user accounts that are logical, not physically, linked to individuals, Angelopoulou, Thomas, Xynos, and Tryfonas (2007). Forensic extraction and analysis of data from a computer hard disk will detail much of this information. However, the conversion of data to evidence is a lengthy and costly process that, at the end of the process, has also to be made understandable to a jury. Therefore, there would be value in creating an analytical framework to facilitate the investigation of internet identity theft cases and the handling of the related digital evidence. The construction of a formalised and structured approach that would assist the computer forensic investigative practice in terms of identification of evidence, presentation in a court of law, among other things. presents an opportunity for further research.

Towards such a direction; types of threats have been combined against on-line identities to achieve illegitimate gains based on the research of the literature up to now. There is an initial attempt to identify and record any digital evidence that may be found per category. Other factors of concern for an investigation are also recorded, such as the required skills and capability profile of the perpetrator, among others. Forensics professionals could then refer to this when they have to examine a case concerning online ID theft. The main idea is that the professional will be able to identify and understand the nature of the crime scene in the future through such a systematic analytical framework, Angelopoulou *et al.* (2007).

FINGERPRINT IDENTIFICATION TECHNOLOGY APPLICATION

Fingerprinting is a branch of forensic science that differentiates between the distinctive patterns of ridges and valleys that flow across fingertips. These ridges and valleys are formed while in the womb and are the product of a matchless combination of hereditary and environmental factors. Fingerprints are statistically unique and never change. For decades, forensic scientists used the Henry system to manually distinguish between billions of known prints using three basic fingerprint patterns: arch, loop, and whorl. Today the process is predominantly computerised and therefore, fingerprinting is an ideal identity verification method. The fingerprint identification process functions when "a fingerprint of unknown ownership is matched against a database of unknown fingerprints to associate crime with an identity". Thus, a person's identity is verifiable upon a comparison of two sets of fingerprints; one set stored and previously matched to the individual, and another set offered at the time of verification. The computer verifies an individual's identity when the two sets of prints are a statistical match. The use of fingerprints as an identification device is already in wide circulation, primarily as a law enforcement tool and for registration of aliens with Citizenship and Immigration Services (i.e. formerly the Immigration and Naturalisation Service). The recent presence of certain factors makes this technology realistically adaptable for widespread commercial use. These factors include "small and inexpensive fingerprint capture devices, fast computing hardware, recognition rate and speed to meet the needs of many applications, the explosive growth of network and internet transactions, and the heightened awareness of the need for ease-of-use as an essential component of reliable security" (Heller, 2008).

RETINAL SCAN IDENTIFICATION TECHNOLOGY

A Retinal Scan photographs the inside of the human eye for identity verification. The scan studies the layer of blood vessels located in the back of the eye using a "low-intensity light source and an optical coupler and can read patterns at a great level of accuracy." The eye has unique characteristics that make a scan reliable, long-lasting, and difficult to counterfeit. For example, the eye does not change between birth and death, and because the retina is located inside of the eye, it is protected from variations "caused by exposure to the external environment." Just like fingerprints, retinal scan technology verifies an individual's identity by comparing a current digital image of the retina with one previously filed and stored. Hundreds of distinctive ocular characteristics are quantified in a retinal scan to identify an individual. Because of its high cost, it is predominantly used in "high-security government installations," including nuclear research sites and military bases.

USE OF BIOMETRICS

Heller (2008) mentions that the elimination of human error is the most striking advantage of both methods. The current system of identity verification relies upon disclosure of numerous pieces of personal information. Frequently, the system breaks down when a verifying employee fails to notice discrepancies contained in personal data offered by a thief. For example; in *Stafford v. Cross Country Bank*, the thief obtained a credit card in the victim's name by correctly listing the victim's social security number and mother's maiden name, but listing an incorrect home address, and in *Patrick v. Union State Bank,* despite an inability to provide a home address, social security number, or even a full signature, a lost driver's license was enough to open a checking account in the victim's name. Bio-verification would protect identity integrity if it were used before extensions of credit and cashless transactions occur.

In the future, Heller (2008) went on to suggests that social security and credit card numbers may even become obsolete in a world where bio-verification is broadly implemented. A unique retinal make up can become a social security card number, credit card number, bank account number, and driver's license all rolled up into one secure instrument. Without access to this information, identity thieves will have nothing to left to steal. The key to biometric success is widespread adoption. Consumers must be able to present themselves for verification conveniently and quickly. As with credit card sliders, fingerprint and retinal scanners must be available for use in financial institutions and at all points of sale. Critics might argue that this method will stifle the use of the internet to conduct commercial transactions because consumers cannot be expected to make the effort to purchase these scanners for in-home use and the elimination of credit card numbers would injure the relatively new medium. However, this point of view fails to take into account two important factors. First, the internet is a marketplace that will be used for many decades to come. Consumers treasure electronic-commerce because thousands of merchants and products are available with just the click of a mouse. However, electronic-commerce can reasonably be expected to adapt to whatever security measures are thrust upon it. Second, and most importantly, consumers will probably not have to purchase the scanners, at least not explicitly. The scanners could become integrated into personal computers and laptops. The International Business Machines Corporation (IBM) already sells biometric scanners built into its laptops as a security measure. Whereas add-on security devices could reach prices up to $200 (R2744.00) just two years ago, a modern integrated biometric scanner can cost just $30 (R411.60), or 2.5% of a $1,168 (R16023.91) laptop. Weighed against the financial and emotional costs associated with a stolen identity, $30 (R411.60) for total identity security is a bargain (Heller, 2008).

Furthermore, (Heller, 2008) provides that biometrics is not the enemy of privacy that critics make it out to be. Their argument goes something like this: the use of biometrics requires a large centrally controlled database that might be misused by those entities entrusted to act as custodians. Proponents of this viewpoint fear that if centrally stored, digital fingerprints or retinal scans might be subject to electronic monitoring and surveillance. Luckily, the use of biometrics for identity security does not contemplate any central storage of data. Simply, encrypted biometric data would be stored on the credit card and function as a "lock." The card (and its corresponding bank account) could be "unlocked" and used for purchases as long as the individual presenting the card can verify her identity by matching the stored fingerprint or retinal scan. Verification would then be a straightforward procedure. Either the scan would present a match with what was scored or it does not; the card could only function with a match because no third party, including the cashier, would have access to the biometric data, it could not be misused. This technology is already being utilised. Walt Disney World uses finger scans to match visitors to their admission passes and in the wake of the terrorist attacks on

September 11, 2001, admittance to the Statue of Liberty in New York (NY) is conditioned upon leaving bags and recording equipment in lockers that can only be accessed with fingerprints. The ATM cash machines and debit cards operate similarly; both rely upon two layers of security: a physical card and a secure password for account access. Instead of a Personal Identification Number (PIN), the second layer of security here is a biometric scan. Despite its potential to change the way the USA deals in cashless transactions, bio-verification technology will take many years to become widely adopted if left on its own. Too many variables may stall or divert its ability to protect the American people from identity-related frauds. Although the technology exists and is reliable, it is still comparatively expensive. The investment must be made in mass production to bring bio-verification to the forefront of the war on ID theft. To implement a change, Congress must support investment through bio-verification incentives (Heller, 2008).

Biometric technologies have the potential to provide convincing evidence of who performs a given financial transaction because each person's biometric characteristics are thought to be unique and difficult to reproduce. Biometric technologies work by measuring and analysing human physiological or behavioural characteristics. Physiological characteristics are those associated with a part of the body. The fingerprint is probably the best-known example; however, face and hand shape, and retina and iris patterns are also examples of physiological characteristics. Behavioural characteristics are based on data derived from a person's actions. For example, the way a person speaks writes (*i.e.* forms characters and words), or types are examples of behavioural characteristics. Biometric traits are less susceptible to duplication or loss when compared to other authentication methods and, therefore, provide a higher level of security. Unlike conventional identification methods that use something you have, such as a credit card or something you know such as a password or PIN biometric characteristics are integral to something you are (Department of the Treasury, 2005).

Perhaps the most prevalent current use of biometrics is in the area of physical access control systems that limit access to highly sensitive areas to authorised people. However, as with almost any security device, biometrics are not perfect and the technology may be impacted when environmental and physical conditions are not ideal (I.e. injury to a finger or hand, or the presence of dust on scanning devices). These conditions and the impact on user acceptance will be discussed later in the report. The primary biometric technologies in use today and supported by commercial industries are finger scan, which considers both the fingerprint and finger shape; face and hand geometry; and iris, retina, voice, and signature recognition systems. According to feedback and comments received, fingerprint technologies comprise half of the biometric technology in use. Theoretically, when biometric technologies are used, the need to remember and protect passwords, PINs, or other secrets may be eliminated. If properly implemented, biometric systems prevent the sharing of secrets that could be used fraudulently. For example, customers would no longer need to share private, sensitive, or personal information with cashiers, customer representatives, or other financial institution employees while conducting a routine business transaction.

ASSOCIATED CHALLENGES OF FORENSIC TECHNOLOGY IN RESPONDING TO IDENTITY DOCUMENT THEFT

Many law enforcement agencies routinely respond to reports of financial crimes and ID theft, but their efforts are hampered by a lack of resources and other challenges including the complexity and cross-jurisdictional nature of these cases and difficulty identifying perpetrators. Adding to this, this author goes on to state that while the law enforcement agencies in most countries are engaged in efforts to prevent and investigate these crimes, more could be done to improve current efforts. With proper law enforcement training and resources, public education efforts, useful victim materials, and referrals, and enhanced cross-jurisdictional collaboration, law enforcement could significantly improve its financial crimes and identity theft outcomes (Buskovick, 2013). Adding to these challenges, the lack of well-trained Investigating Officers (IOs) in responding to this kind of crime in nature is a contributing factor to the law enforcement agencies regarding responding to ID theft. Resources may be available, however, if the IOs are not in a position to utilise them properly, responding to ID theft will remain a challenge. Henceforth, because the matured way of responding to ID theft is to combat it before the actual objective is achieved, the public needs to be well informed of preventative measures. Furthermore, laws dealing with ID theft, in particular, should be drafted, as it is currently dealt with under common law in South Africa, which poses a great challenge in prosecuting the crime of ID theft.

FORENSIC TECHNOLOGY MODELS TO IMPROVE THE LAW ENFORCEMENT RESPONSE TO IDENTITY DOCUMENT THEFT

Education through Community Outreach

Many victims may not know what to do once they discover that they have been victimised, or that swift action on their part may minimise the damage done. Local police, as part of their outreach programmes, may help in educating consumers concerning these matters and steps they can take both to avoid their victimisation and to report their victimisation should it occur. Many police departments now have information on their web sites and some offer online ways of reporting victimisation. Directing victims to internet resources or providing them written materials that explain how the recovery process works may help in reducing victim's suffering, Albrecht, Albrecht, and Tzafrir (2011). In support of this statement, when considering the current state of police partnership with the public in South Africa, the researchers are of the perception that it will take more than community will outreach programmes by police to indeed educate the public about ID theft. This is simply based on the researchers' observations that the partnership between the public and the SAPS has gradually been dented, and to convey information regarding ID theft, police will first have to ensure that the public trust in their services is gained. The public needs to understand that police existence in their community is to uphold the law and maintain security, and this can only be done if the number of police corrupt cases maybe, if possible combated.

Effective Communication

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

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

Acknowledging the Crisis (Identity Document Theft) Response Plan

If a major theft of an agency's database of customer or employee records occurs, the business or agency must have in place a crisis response plan that will minimise the effects on potential victims. Such a plan would usually include:

Toll-free dedicated phone lines for employees to call the three major credit bureaus to warn of the theft; and information packets should be distributed to potential victims on what to do, to protect their identities, and to reduce damage, Newman, and McNally (2005).

In the researchers' views, this plan can only be effective if the concerned businesses have the records of their consumers' identifying documents on their systems and provided, such systems are consistently monitored. This may assist in determining the time, location of the suspects, and further help in apprehending the offenders.

MATERIALS AND METHODS

Research design is defined as a plan through which the principal researcher adopts to engage with research participants or subjects to collect information from them (Welman and Kruger, 2001). In connection with this definition, this research design further refers to the process of focusing your perspective on a particular study." The researchers followed a case study research design, De Vos, Strydom, Fouché, and Delport (2011). This choice was because the type of design allowed the researchers to explore and understand ID theft as it is a complex societal issue. Through the case study method, the researchers were able to go beyond the quantitative statistical results and understand the concept of ID theft through interaction with the respondents. The researchers adopted a quantitative research approach for this study. The reason for adopting this method was to endeavor to answer questions about relationships among measured variables to explain, predict, and controlling phenomena. Furthermore, this method assisted the researchers in displaying and categorising the precise results of this study, mostly because numbers form the fundamental representation of data, Leedy and Ormrod (2005). Through this approach, in-depth knowledge of how the SAPS responds to ID theft was acquired. For data collection**,** the researchers utilised two scientific methods to collect data. Primary data were collected through the use of questionnaires consisting of forty-one (41) statements to collect primary data. The researchers intended to determine the extent to which the respondents agreed or disagreed with the given statements, particularly concerning existing challenges in response to ID theft. Secondary data were collected through consultation of literature including relevant journal articles, published dissertations, and theses, legislations, statistics, monographs published by the Institute for Security Studies (ISS), articles from accredited scientific journals, and media articles relevant to the matter under investigation.

STUDY DISCUSSION AND RESULTS

The Use of Forensic Technology in Preventing Identity Document Theft and its Challenges

This section seeks to explore the use of forensic technology by the local SAPS, with the inclusion of the public. This is deemed as one of the preventative measures to be adopted by these stakeholders in the Polokwane area to effectively prevent ID theft. The data for partnership policing is presented in Table **1**, followed by the identified challenges in terms of applications, as shown in Figures **1** to **4**, as well as the response time in Table **2** of this study. The statements in the questionnaire measure the local SAPS challenges in responding to ID theft while applying forensic methods in the selected areas of Limpopo Province.

To represent larger sample representations', the researchers targeted the local SAPS officials, as attached to the Polokwane Police Station, varying from respective components, the 'Managers' of various stores within the Polokwane inner city, as well as members of the public members. This selection was based on daily basis exposure to the incidences of ID theft. As a result, their experiences were of great value to this study. According to the sampling guidelines provided for by De Vos *et al.* (2011:225), 45 respondents from a targeted population of 100, is sufficient to draw reliable results. This study initially targeted 130 ideal populations, however, only 90 respondents correctly completed the distributed questionnaires, and the other 40 were disqualified due to errors and non-completions. In this light; 90 respondents were sufficient to draw reliable results from as supported by De Vos *et al.* (2011:225).

The presented percentages in Table **1** are measured against the total population of 90 respondents. Data presented in Table **1** indicate that the majority of the respondents agreed with statement 1. It is clear that 38 percent agreed, 17 percent strongly agreed, 22 percent did not know, 13 percent disagreed while 9 percent strongly disagreed. Concerning statement 2, data show that 47 percent agree, 36 percent strongly agreed, 10 percent did not know and only 4 percent disagreed and 3 percent strongly disagreed. Furthermore, the results have shown that concerning statement 3, there was 11 percent of respondents who agreed, 28 percent strongly agreed, and 33 percent did not know. While on the other hand, 21 percent disagreed and only 7 percent strongly disagreed. Statement 4 also received an overwhelming response as 32 percent agreed, 45 percent strongly agreed, 11 percent did not know and 8 percent disagreed, whilst 4 percent strongly disagreed.

Table 1: Partnership Policing (N=90)

No.	Statements	Agree	Strongly Agree	I do not know	Disagree	Strongly Disagree
1.	The police-public partnership is well structured in my area	34 (38%)	15 (17%)	20 (22%)	13 (14%)	8 (9%)
2.	Community police partnership can alleviate identity theft in my area	42 (47%)	32 (36%)	9 (10%)	4 (4%)	3 (3%)
3.	The local police are working together with the community in my area to address identity theft	10 (11%)	25 (28%)	30 (33%)	19 (21%)	6 (7%)
4.	The existence of a partnership between Immigration Officers (Department of Home Affairs) and the police may deter the incidents of identity theft	29 (32%)	40 (44%)	10 (11%)	7 (8%)	4 (4%)

The findings have shown that a strong partnership between SAPS and DHA would probably minimise ID theft. This can be seen by the majority of the respondents (72%) who agreed with statement 4. To support this finding, partnership policing has provided positive results that directly impact the quality of life of local people and reduced crime in most areas in South Africa (Burger, 2007). Investigating ID theft can be very challenging for law enforcement. Figures **1** to **4** below presents the results on challenges facing police officials in Polokwane to effectively respond to ID theft. These figures incorporate section E of the questionnaire. The results in Figures **1** and **3** reflect the perceptions of police officials, except Figure **2** (which reflects the total population) and Figure **4** (which reflects only of the public respondents). The researchers found it significant to present only the results of police respondents, as they were the actual people experiencing these challenges in their attempt to respond to ID theft. With this in mind, the researchers further believe that the results present the true reflection of how these challenges may hinder police response to ID theft.

Only SAPS respondents were assessed on the methods of operation used by ID thieves as a challenge. The reason for analysing the responses of the SAPS members only was that SAPS investigate this crime whenever it is reported to them and not the victim and as such, would provide accurate and reliable responses to this statement. The respondents were divided in terms of their ranks. When asked whether the secretive nature of ID theft poses a challenge they when investigating ID theft 2% of Captains agreed that how ID thieves operate is a challenge when responding to this crime and 3% strongly agreed. On the rank of Constables, 20% agreed, 17% strongly agreed whereas 3% disagreed and 10% did not any carry knowledge. Data further depict that 3% of Lieutenant (Lit), Colonel (Col), accepted the secretive nature of ID theft to be a challenge; similarly, the other 3% disagreed and 10% were unknowledgeable. The results also show that 3% of Sergeants agreed and 7% strongly agreed, while 3% did not know. To conclude with Warrant Officers (WOs), it is clear that 7% agreed and an additional 3% strongly agreed with this view. Amongst the ranks, the results have indicated that Constables (31%) are constantly attending to cases of ID theft and they may be a very valuable staff who better understand or need to be trained on how ID thieves operate. This finding also suggests that SAPS has a lot of Constables as operational staff. Over two-thirds of police officials (65%), have considered the secretive nature of ID theft as the most challenge that the police are faced with when responding to this crime. Other authors have stipulated other secretive ways in which ID thieves operate. The authors mentioned that:

- ID thieves hack into corporate computers and steal customer and employee databases, then sell them on the black market or extort money from for their return.
- They buy IDs on the street for the going rate or buy IDs that may be either counterfeit or stolen.
- Buy counterfeit documents such as birth certificates, visas, or passports (Newman and McNally, 2005).

The truth to the above-mentioned facts is, when ID thieves carry out these duties, they predominantly find themselves unmonitored and the victims not knowing what the perpetrators are up to until his/ her name has been dented. Police on the other, find themselves being more reactive than proactive, which contributes to the difficulty of locating the perpetrator in the process of investigation as the crime would have long been committed.

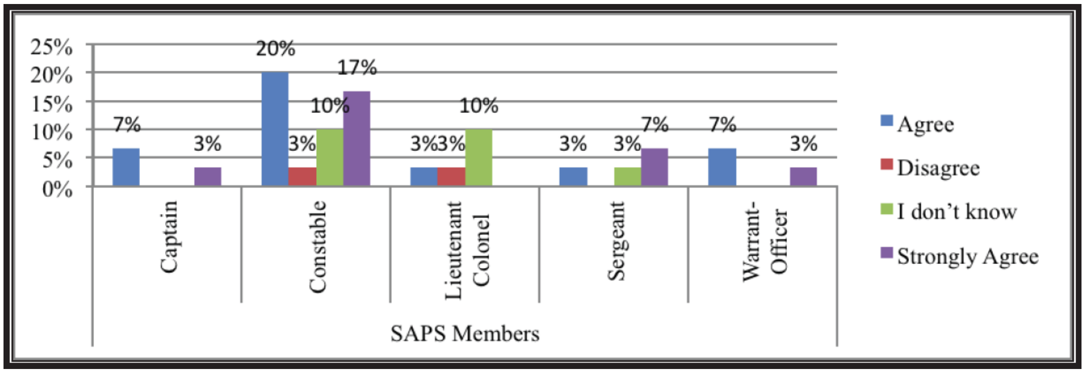

Figure 1: Secretive nature of identity theft (N=30).

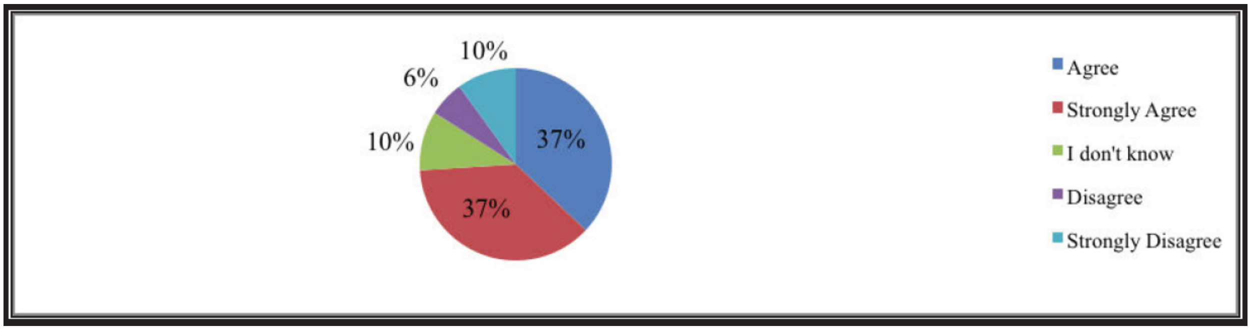

Figure 2: Poor public-police partnership (N=90).

The respondents were asked if a poor public and police partnership can be regarded as a challenge for SAPS to respond effectively to ID theft. The results indicate that 37 percent agreed that poor public and police partnership has an impact on promoting ID theft activities and equally, 37 percent strongly agreed. Furthermore, data depict that 6 percent disagreed, while 10 percent of the police respondents strongly disagreed. Other groups of the respondents, which constitute 10 percent, did not know.

From these results, it can be deduced that the majority of the respondents (74 percent) agreed that police partnership with the community in Polokwane, in as much as addressing ID theft is concerned, is not well structured. Although 16 percent of the respondents disagreed, there were still those who did not know (10 percent) whether the police partnership with the public is well convincing to adequately combat ID theft or not. It is evident from the results that without the cooperation of the public, investigating ID theft would become essentially unworkable. In simple terms, the police service would cease to function without the active support of the communities it serves. Evidence from the findings alternatively shows that effective community engagement and collaborative problem solving can significantly minimise challenges faced by SAPS in responding to ID theft activities.

Officials were asked whether a lack of resources is likely to hamper their response to ID theft cases. From the data presented above, police respondents were categorised in ranks. Figure **3** sets out that 7% of Captains agreed while 3% disagreed. 10% of Constables agreed and supporting their views were the other 27%, while 7% disagreed, and similarly, 7% did not know. To continue, the results show that 3% of Lieutenant Colonels agreed and 10% strongly agreed, while another 3% did not know. Sergeants have also expressed their views and it can be seen from the results that 7% agreed and 3% disagreed. The results further show that 3% of WOs agreed, while 3% disagreed, and the other 3% strongly disagreed. There appeared to be a larger agreement that without police being adequately equipped, responding to ID theft will remain a challenge. The majority of respondents (64%) indicated that the unavailability of resources to put toward the investigations of ID theft affects how they respond to this crime. Nineteen percent of the respondents, on the other hand, appeared to agree that with or without adequate resources, ID theft can be effectively responded to. Taking into account the low levels of economic status that South Africa is currently facing, it cannot be argued that most of the government institutions are not adequately resourced to deliver as expected, with the SAPS being amongst such. With slightly more than two thirds (64%) of the SAPS

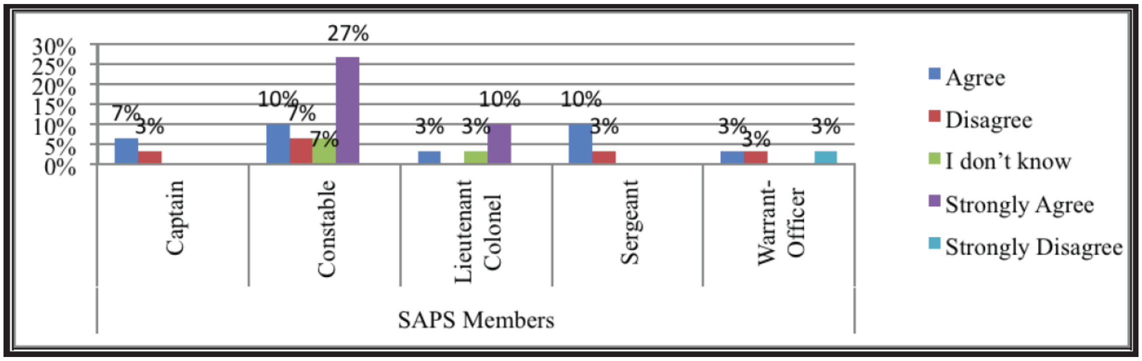

Figure 3: Lack of resources (N=30).

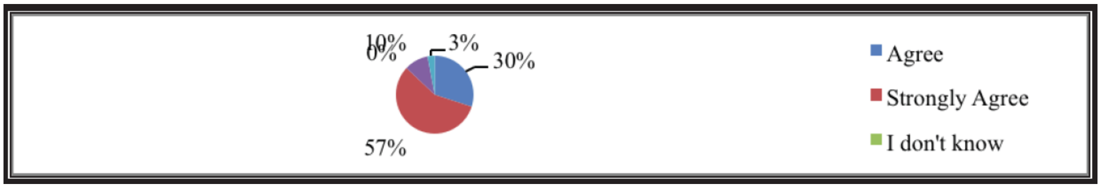

Figure 4: Influx of foreign nationals into the city (N=30).

members indicating that they do not have sufficient resources to work with, it is clear that they will fail to identify ID theft threats, develop intelligence and use the available resources to effectively root out ID thieves. Evidence in this study has shown that investigating ID theft is challenging, in that it sometimes involves using the most sophisticated covert techniques and with a lack of resources at police's disposal, it will even be more challenging to catch the perpetrator.

Police respondents were also assessed on the view of whether the flow of foreign nationals into the city of Polokwane may be one of their challenges. The results as indicated above show that 9 in 30 respondents (30 percent) agreed with the statement that the immigration of foreign nationals into the city posed a challenge in their response to ID theft, and 17 in 30 of these respondents (57 percent) strongly agreed with this view. On the other hand, 10 percent (3) disagreed and only 3 percent (1) strongly disagreed. A large proportion of police respondents (87 percent) viewed the immigration flow of foreign nations in the province and the city contributing to their challenges in responding to ID theft. This finding suggests that the security measures at a port of entry in the Limpopo Province are weakened, with high possibilities that some of the perpetrators reported to be foreigners. In such cases, it could even make it worse to locate or apprehend the suspect.

Table **2** addresses the statement from the questionnaire. This section is aimed at measuring the time which the SAPS members take to respond to cases of ID theft. Thus, the researchers found it most prevalent to utilise this section to present the results of the public respondents since it is this group that reports and calls upon SAPS to attend to cases of ID theft. As such, Table **2** reflects only the perceptions of public respondents comprised of 60 respondents.

The findings depicted in Table **2** suggested the period, which the SAPS takes to respond to ID theft and how they respond. Concerning statement 5, slightly more than one third (35%) of the respondents are of the view that the SAPS is effectively responding to ID theft. Based on this finding, it is clear that those, whose identities were dented or have been rescued through the assistance of the SAPS were satisfied with how their cases were handled. Furthermore, this may suggest that perpetrators of this crime have been apprehended and brought before the court of law for prosecution. Conversely, an equal number of respondents (35%) have found SAPS not being effective when investigating ID theft. These individuals may have been victims of ID theft or know someone whose identity has been victimised, and SAPS has not been successful in investigating their cases. There is a significant difference between the respondents who did not know (30%) and those who considered SAPS to be effective and ineffective when responding to ID theft. This difference creates a belief that how SAPS handles cases of ID theft is not as convincing as the public expected.

In respect of statement 6, exactly one third (30%) stated that SAPS respond timeously to ID theft while only 25% did not agree with the statement. This finding

Table 2: Responding Time (N=60)

No.	Statement	Agree	Strongly Agree	I do not know	Disagree	Strongly Disagree
5	The local police are effectively responding to the crime of identity theft	15 (25%)	6 (10%)	18 (30%)	11 (18%)	10 (17%)
6	The local police timeously respond to identity theft cases	12 (20%)	6 (10%)	27 (45%)	11 (18%)	4 (7%)
7	The local police currently have effective measures to curb identity theft timeously	13 (22%)	6 (10%)	27 (45%)	6 (10%)	8 (13%)

indicates that SAPS has investigated some cases of ID theft and the complainants have received feedback into their matter within a reasonable time while there is an existing possibility that there are extended delays in some cases. An overwhelming 45% of the respondents did not know whether SAPS respond to ID theft timeously. From this finding, it can be deduced that many of those who report ID theft, do not make follow-ups regarding their cases.

Relatedly, 45% of the respondents did not know if SAPS has effective measures in place that would assist them to timeously respond to ID theft. It can also be seen from the results that effectiveness in responding to this crime is skeptical since the majority of the population carried no knowledge of the subject matter, while on the other hand, slightly more than one third (32%) indicated that there are measures in place to effectively deal with ID theft cases within a reasonable time. What constitutes a reasonable time in ID theft cases will depend on the nature and scope of each case. This finding indicates that SAPS may be having effective plans in place to react to ID theft timeously however; there may be a lack of well-informed staff to implement and effectively follow such measures. Few of the respondents (23%) disagreed with this statement and this may be a sign that there is a lack of time dedicated to ID theft cases. The truth of the matter is, it can take months, even years, to resolve ID theft and the victim may not be able to recover any money involved.

For further emphasises, economic crime is a serious challenge for business leaders, government officials, and private individuals in South Africa. An unbelievable 69% of South African respondents to the survey indicated that they had been subjected to some form of economic crime in the 24 months preceding the survey, compared to 37% of global respondents. In 2013, South Africans lost more than R2.2billion, according to the SABRIC (Beetar, 2014) and meanwhile, data from the Southern African Fraud Prevention Service (SAFPS) revealed that the number of ID theft cases reported by the end of April 2014 increased 16% year-on-year. This is only the tip of the iceberg as many frauds still go undetected in the absence of more effective fraud prevention systems. The findings have shown that police partnership with the community and the DHA will assist in reducing ID theft. This is supported by 72% of the population majority who agreed that a well-structured police partnership with the DHA will assist in detecting and deterring ID theft, meanwhile, 74% of police officials indicated that poor partnership with the public impact negatively on responding to ID theft cases.

The findings have also indicated that the secretive nature of patterns involved in committing ID theft poses a serious challenge for the police to respond to this crime. 65% of SAPS officials have acknowledged that the secretive nature of ID theft is a challenge. To support this finding, the literature indicates that offenders may also use high tech methods via computers and/or the internet to obtain personal information that is seemingly unprotected by the victim. The prevalence of electronic commerce and financial services that enable access to sensitive personal data, such as bank records and identity data have significantly increased the opportunities offenders have to engage in high tech identity theft and fraud. Businesses and financial institutions store sensitive customer information in massive electronic databases that can be accessed and compromised by hackers (Holt and Turner, 2012).

The immigration of neighbouring nationals into the city was, as well, accepted by the SAPS officials to be one of the challenges relating to their response to ID theft cases. The findings have indicated that 87% of the sampled SAPS officials regarded the influx flow of neighbouring nationals into the city as one of the challenges. Previous research also shares the same light concerning this view. It was found that the increased mobility of individuals, facilitated by cheap air travel, also presents further opportunities for immigration-related fraud, passport forgery, and abuse of travel-related ID theft (Robinson, Graux, Parrilli, Klautzer and Valeri, 2011). Most importantly, the unavailability of sufficient resources was considered a challenge for SAPS. The findings of this study have indicated that 64% of the sampled SAPS officials indicated the lack of resources as a challenge. In reality, most police stations do not have the resources to investigate ID theft, but many also do not understand that they need to do a better job of explaining this to the victims who arrive on their doorstep desperately looking for help.

CONCLUSION AND RECOMMENDATIONS

It is concluded that ID theft is one of the fastest-growing [silent] crimes in the world, with identity thieves' intelligence growing rapidly, contributing positively to fraud, involving stealing money, or gaining other benefits by acquiring Personal Information and impersonate such individual. This crime does not discriminate and it can occur whether the victim is alive or deceased, not considering the age, criminals often use Personal Information to assume an individual's identity and acquire retail or bank accounts, or even defraud insurance, medical aid, and Unemployment Insurance Fund (UIF). In some instances, perpetrators visit banks and make transactions on existing accounts, with impersonation. Some of the consequence ranges from emotional to direct impact financially, making it mountainous for victims to obtain loans, credit cards or a mortgage until the ID is located or replaced to resolve the matter., or even defraud your insurance, medical aid, and UIF. In some instances, perpetrators go to your bank and make transactions on your accounts while impersonating you.

This study further concluded that several themes emerged from this study, many of which confirm the need for police to keep up to date with technology, many of which indicating the need for continued and enhanced attention to be paid towards this crime. There is no magic bullet that will eradicate identity theft. To successfully respond to ID theft and its effects, we (i.e. the local police and other relevant stakeholders) must keep personal information out of the hands of thieves; take steps to prevent an identity thief from misusing any data that may end up in his hands; prosecute him vigorously if he succeeds in committing the crime, and do all we can to help the victims recover. Only a comprehensive and fully coordinated strategy to combat identity theft one that encompasses effective prevention, public awareness, and education, victim assistance, and law enforcement measures, and that fully engages federal, state, and local authorities and the private sector will have any chance of solving the problem. This proposed strategic plan strives to set out such a comprehensive approach to combating identity theft, but it is only the beginning. Each of the stakeholders, consumers, business, and government must fully and actively participate in this fight for us to succeed and must stay attuned to emerging trends to adapt and respond to developing threats to consumer wellbeing.

For recommendations, the preventative measures and challenges faced should be addressed as follows by the relevant stakeholders (i.e. SAPS as the primary gatekeeper of ID investigations):

- The existence of a strong partnership between SAPS, Polokwane residents, and other government institutions can help to prevent ID theft.
- Because of poor public and police partnership, this imposes difficulties for SAPS members to obtain information from Internet service providers, banks, stores, and other financial institutions.
- The complexity of ID theft and the fact that this crime very often crosses jurisdictional boundaries create challenges for SAPS and thus there is a need to collaborate and share information with the community so as to increase investigative capacity.
- Modern ways of stealing IDs, specifically through the internet, make it difficult for SAPS members to investigate and identify perpetrators.
- Among the SAPS ranking structure of the respondents, the majority of SAPS Constables were found responding to this crime more frequently than others. Therefore, a lack of experience or expertise in how to investigate ID theft is a challenge.
- Lack of resources to investigate this crime is without a doubt, a serious challenge.
- Notably, it can be concluded that there are no full-time investigators for this crime, and investigations are shared amongst available limited staff.
- Concerning the influx flow of foreign nationals into the city, a serious challenge is that it is likely that often the perpetrators are from another country or province.
- With the majority of the respondents not knowing how long SAPS takes to respond to ID theft cases, an objective conclusion can be reached to say that such cases are either not reported and if reported, it takes quite a long time to effectively respond to this crime.

ID theft is a multi-faceted problem for which there is no simple solution. Because identity theft has several stages in its “life cycle,” it must be attacked at each of those stages, including:

- When the identity thief attempts to acquire a victim’s personal information.
- When the thief attempts to misuse the information he has acquired.
- After an identity thief has completed his crime and is enjoying the benefits, while the victim is realising the harm (Federal Trade Commission, 2007).

The federal government’s strategy to combat identity theft must address each of these stages by:

- Keeping sensitive consumer data out of the hands of identity thieves in the first place through better data security and by educating consumers on how to protect it.
- Making it more difficult for identity thieves, when they can obtain consumer data, to use the information to steal identities.
- Assisting victims in recovering from the crime.
- Deterring identity theft by aggressively prosecuting and punishing those who commit the crime (Federal Trade Commission).

A great deal already is being done to combat identity theft, but there are several areas in which we can improve. The Task Force’s recommendations, as described below, are focused on those areas.

With this study, the researchers recommend that the SAPS in Polokwane should invest the time and expense in preparing their officers to provide a quality response (investigation) to the public when investigating ID theft cases. Most of the operational staff who are tasked in responding to the initial report should be trained in how ID theft occurs, how it impacts victims, how to prevent it, and ways to recover from it. The detective unit should be encouraged to develop contacts and alliances within the Polokwane local business community and the major financial institutions. The feasible ideas suggested by affected groups include the increased protection of personal information, through greater use of biometrics and increased public awareness. This author made the following suggestions (Allison, 2003):

- The greater use of forensic technology, such as ‘*biometrics*,’ gives better protection to an individual's IDs from being assumed by imposters. This technology uses a physical trait on an individual as a means of verification, effectively eliminating the need for personal information, "…the dream of many security experts is using biometrics, a technology that can identify people from some unique physical trait." The use of biometrics is nothing new; many government agencies maintain their security with it. The cheapest and most widely used form of biometric verification is a fingerprint scanner. This device is not only used by law enforcement for criminal investigations but also has wider applications of access control to buildings, computer terminals, bank accounts, among others. Biometric technology can monitor the actions of its users and so could become an invasion of an individual's privacy. When evaluating the pros and cons of employing more technology to combat crime, this author believes that taking such an approach is a costly and more importantly temporary solution.
- The second suggestion was proposed by officials in both private and government agencies that deal with ID theft all of whom have stated that one of the best forms of prevention is greater awareness among the population. It seems logical to reason that increased education of the public would have a long term effect of reducing some of the opportunities for identity thieves, especially those who employ low-tech methods for obtaining the necessary information.

The researchers, therefore, recommend that SAPS should encourage local businesses, merchants, in particular, to use a biometric system when selling their products via accounts or when providing services that require the use of an ID.

In conducting public awareness, it is recommended that SAPS should, inter alia, in their awareness campaign, admonish the public on how to protect themselves against ID theft. Therefore, people should do the following to avoid becoming victims (McLoughlin, 2015):

- Before revealing any personally identifying information, people should find out how it will be used and shared. If it will be used or shared in a way that makes them uncomfortable, they should ask if they have an alternative.
- Pay attention to your billing cycles to be sure that its bills arrive on time.
- Put passwords on a credit card, bank, and phone accounts.
- Avoid using easily available information like mother's maiden name, birth date, or phone number.
- Keep a record of all credit card account numbers, expiration dates, and the telephone numbers and addresses of each creditor.
- Minimise the identification information and the number of cards they carry.

- Do not give out personal information on the internet unless they have initiated the contact or know whom they are dealing with.

The researchers further recommend that SAPS corroborate and partner with the communities, DHA, merchants, and financial institutions. This corroboration and partnership will assist SAPS in ensuring that these institutions always make information available to them whenever they need it. These relationships can be formed through the persuasion of the following avenues:

- Facilitating meetings between financial institutions, merchants, and investigators of ID theft in SAPS.

- Using these meetings to share information and intelligence pertinent to investigations and current trends in ID theft crime.

Training of officials on how to investigate Internet committed crimes (cybercrimes) should be considered in Polokwane. In conclusion, SAPS should work together with the DHA to strengthen border policing at all Limpopo's entry ports. Consequently, the use of forensic technology to combat ID theft by Polokwane SAPS pose invisible challenges. The integration of technological and conventional measures currently falls short in response, calling for extensive training, intergovernmental relations and public awareness to be staged by responsible SAPS officials, DHA, and other relevant stakeholders as advanced knowledge and resources geared on committing ID theft by applying vast technologies present severe challenges to proactive and reactive initiatives shown by these stakeholders.

REFERENCES

Albrecht, C., Albrecht, C, and Tzafrir, S. 2011. How to protect and minimise consumer risk to identity theft. *Journal of Financial Crime,* 18(4): 405- 414. https://doi.org/10.1108/13590791111173722

Allison, SFH. 2003. A case study of identity theft. Masters of Arts Dissertation. United States: University of South Florida.

Angelopoulou, O. 2007. ID Theft: A computer forensics' investigation framework. Perth Western Australia: Edith Cowan University.

Angelopoulou, O., Thomas, P., Xynos, K, and Tryfonas, T. 2007. Online ID theft techniques, investigation, and response. *International. Journal of Electronic Security and Digital Forensics*, 1(1):76-88. https://doi.org/10.1504/IJESDF.2007.013594

Beetar, M. 2014. SA companies' fraud stats lead the world. Available at: http://www.bdlive.co.za/business/2014/12/10/sa-companies-fraud-stats-lead-the-world.

Burger, J. 2007. Strategic Perspectives on Crime and Policing in South Africa. Hartfield: Van Schaik Publishers.

Buskovick, D. 2013. Financial crime and identity theft: Law enforcement response, challenges, and resource needs. The United States. Report of Minnesota Law Enforcement Identity Theft Survey, Minnesota Department of Public Safety.

Department of the Treasury. 2005. The Use of Technology to Combat Identity Theft. Report on the study conducted pursuant to section 157 of the Fair and Accurate Credit Transactions Act of 2003. Available at: https://www.hsdl.org/?view&did=482322.

De Vos, AS., Strydom, H., Fouché, CB and Delport, CSL. 2011. Research at Grass Roots, for the social science and human service professions. Hartfield: Van Schaik Publisher.

Federal Trade Commission [Online]. 2007. The President's Identity Theft Task Force: Combating identity theft – Strategic plan. Available at: https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

Heller, I. 2008. How the internet has expanded the threat of financial identity theft, and what congress can do to fix the problem? *Kansas Journal of Law & Public Policy,* 1(9), 83-107.

Holt, TJ and Turner, MG. 2012. Examining Risks and Protective: Factors of On-Line Identity Theft. *An Interdisciplinary Journal,* 33(4): 308-323. https://doi.org/10.1080/01639625.2011.584050

International Association of Chiefs of Police. Sa. A Forensic Approach to Effective Identity Theft Investigations. Available at: http://www.theiacp.org/investigateid/pdf/appendices/A-Forensic-Approach-to-Effective-Identity-Theft-Investigations.pdf.

Leedy, PD and Ormrod, JE. 2005. Practical research: planning and design. New Jersey, Upper Saddle River: Merrill.

McLoughlin, C. (carolm@safps.org.za). 2015. ID theft Statistics. [E-mail to:] Mr. Rakololo WM (moyahabo.rakololo@gmail.com) August 5.

Newman, GR and McNally, MM. 2005. Identity theft literature review. United States: Department of Justice.

Robinson, N., Graux, H., Parrilli, DM., Klautzer, L and Valeri, L. 2011. Comparative study on legislative and non-legislative measures to combat identity theft and identity related crime: final report. United Kingdom: Rand Europe.

Smith, T. 2013. Identity theft. Available at: http://www.bowman.co.za/eZines/Custom/ ...

South African Police Service. 2014. About the Forensic Science Laboratory. Available at: https://www.saps.gov.za/faqdetail.php?fid=6#questiion.

South African Police Service. 2010. Strategic Plan 2010 to 2014. Available at: http://www.saps.gov.za.

Welman, JC and Kruger, SJ. 2001. Research methodology for the business and administration sciences. New York: Oxford University Press.

Received on 06-08-2020 Accepted on 18-09-2020 Published on 01-10-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.62