An evaluation of identification methods used in the investigation of counterfeit card fraud

by

NICOLAAS DC GELDENHUYS

Submitted in part fulfilment of the requirements for the degree of

MAGISTER TECHNOLOGIAE

In the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Dr T Budhram

FEBRUARY 2016

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation towards my supervisor, Dr Trevor Budhram, for his advice and support throughout this study. Your guidance has been invaluable.

To my mother, thank you for your inspiration and encouragement. You have motivated me to make a success of this. To Anita, Jennifer, Neill and Stefan, thank you for your support. I would also like to thank the South African Police Service who granted me permission to access its records and interview members for purposes of the research.

Furthermore, a special word of thanks goes to the Directorate for Priority Crime Investigation, the South African Banking Risk Information Centre, everyone who participated in this study and to Ms Yvonne Smuts and Ms Melissa Davidson, who edited and formatted this report.

DECLARATION OF AUTHENTICITY

I declare that this research dissertation, **An evaluation of identification methods used in the investigation of counterfeit card fraud**, is my own original work and that all sources that I have used or quoted have been indicated and acknowledged by means of complete references. This dissertation is submitted in partial fulfilment of the requirements for the degree of Magister Technologiae in the subject Forensic Investigation at the School of Criminal Justice, College of Law, University of South Africa (Unisa). It has not been submitted before at any other university or tertiary institution.

Nicolaas Daniël Cronjé Geldenhuys

Student number: 37762524

Date: 15 February 2016

ABSTRACT

An evaluation of identification methods used in the investigation of counterfeit card fraud

Today, the use of one's bank card to pay or withdraw money is common. Modern technology provides us with the convenience of instant transactions at the automated teller machine or point of sale but unfortunately, it has also brought the reality and risk of card skimming and counterfeit card fraud. Criminals have become very efficient and technologically advanced in skimming and counterfeiting cards, to such an extent that counterfeit card fraud has become a significant threat to the public, banking, retail and business in South Africa.

Counterfeit card fraud is a complex, multi-faceted crime, requiring specific skills and knowledge of card counterfeiting methods from police and bank investigators. The scope of its investigation is wide. It includes different crime scenes and offenders, sophisticated equipment and various aspects that need to be identified positively. Investigators find it difficult to identify perpetrators and certain aspects unique to this crime and, as a result, many investigations are unsuccessful. This research endeavours to establish what identification methods are available to investigators and which are effective.

KEYWORDS

Card skimming; Commercial crime; Counterfeit card fraud; Evidence; Forensic investigation; Fraud; Identification method.

CERTIFICATE BY EDITOR

I, Yvonne Smuts, hereby declare that I have edited the dissertation **An evaluation of identification methods used in the investigation of counterfeit card fraud** by Nicolaas Daniël Cronjé Geldenhuys, student number: 37762524, for the degree of Magister Technologiae: Forensic Investigation in the School of Criminal Justice, College of Law, at the University of South Africa, and that it adheres to the standard and level of quality set for such a text.

(Ms) Y Smuts

Date: 28 January 2016

Accredited member of the South African Translators' Institute. Membership number 1002242 / Member Prolingua / Member Translators Panel Unisa

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE:
GENERAL ORIENTATION

1.1 INTRODUCTION

Modern technology has brought the convenience of advanced payment instruments and banking systems. Today, paying by bank card has become a popular and widely used method of payment. Carrying a card linked to a debit or credit account at a bank is common, and is regarded as a safe and convenient substitute for cash. People are more inclined to use bank cards as a form of payment, and paying by cash is becoming less prevalent (Visa South Africa, 2012:1). However, the use of bank cards has its shortcomings, namely their vulnerability to fraud, notably counterfeit card fraud.

Counterfeit card fraud arises from the use of a counterfeit card to conduct fraudulent transactions. A counterfeit card is produced illegally by encoding the magnetic strip of a card with card data which is obtained from a valid, bank-issued card (South African Banking Risk Information Centre [Sabric], 2014:18). Card data is obtained through a process of card skimming. Skimming involves the use of an electronic card reader (skimming device) to copy the card data from a valid card without the cardholder's consent (Sabric, 2014:19; 2012:19 & 30). Card skimming and the possession, selling or distribution of skimming devices with criminal intent, are illegal.

The number of cards in circulation and the volumes of transactions going through South African payment systems are significant. By 2011 there were 43 million bank cards in circulation in South Africa (SA) (Schulz & Ruse, 2012:1), while the number of card-based transactions for the period 1 October 2011 to 31 December 2011 totalled 190 million, of which 87 million were automated teller machine (ATM) transactions (Payments Association of South Africa [PASA], 2012a:16-17). In 2013 and 2014, the total losses resulting from counterfeit card fraud in South Africa relating to SA-issued cards were R254,3 million and R205,3 million respectively, and 80%-85% of counterfeit card fraud manifested as cash withdrawals at ATMs (Sabric, 2013c:1-20; 2014:11-18). In 2015, about R130 million was lost as a result of counterfeit card fraud. This figure excludes cards issued in other countries which

were used in South Africa (Sabric, 2015:12-20). On average, about 50% of all card fraud occurs in Gauteng province (Sabric, 2014:13; 2015:10 & 15).

In addition, the recovery of skimming devices over the past number of years illustrates the magnitude and extent of counterfeit card fraud in South Africa (Sabric, 2014:19-22; 2015:21-23). Between 1 January 2015 and 30 September 2015, 78 skimming devices were recovered. It is, therefore, apparent that counterfeit card fraud is a real threat to banks, the business sector and the public.

1.2 PROBLEM STATEMENT

Prior to 6 July 2009, the investigation of counterfeit card fraud was the sole responsibility of the Commercial Crime Unit (CCU) of the South African Police Service (SAPS) (2010a:1-3). However, from 6 July 2009, when the CCU became part of the then newly established Directorate for Priority Crime Investigation (DPCI), the functions and responsibilities of the CCU are regulated by Chapter 6A, read with section 16, of the South African Police Service Act, 1995 (Act No. 68 of 1995).

In 2011/12, the CCU received 5 322 counterfeit card fraud cases for investigation, involving a total actual loss of R144 million (SAPS Annual Report 2011/12). From 2012, the focus of the CCU moved towards the investigation of serious and priority commercial crime, and not all commercial-related crimes. The mandate of the CCU was aligned with relevant statutory prescriptions, a process which included the transfer of the investigation responsibility in respect of single, unrelated counterfeit card fraud cases to station level detectives, while the investigation of serious, organised and syndicate-related counterfeit card fraud cases remained with the CCU (SAPS, 2012a; 2013b; 2013c). From 2012/13 onward, it was not possible to determine the real extent of counterfeit card fraud cases reported to the SAPS. In its annual reports, the SAPS only states the number of counterfeit card fraud cases investigated by the CCU (SAPS Annual Reports 2012/13 to 2014/15). The total number of reported counterfeit card fraud cases is not provided. The SAPS was unable to provide figures for the total number of counterfeit card fraud cases reported between 2013 and 2015.

The responsibilities of the researcher, as an officer attached to the CCU, included docket inspections at CCU investigation units, the investigation of commercial-

related crime, overseeing and managing investigations, and implementing policy and standards for commercial crime investigations. During docket inspections carried out during 2012/13 at the Commercial Crime Unit, Johannesburg, in terms of Standing Order 324, as well as SAPS Head Office directives with reference 26/13/3 dated 16 May 2003 and 14 August 2006 (SAPS, 2003; 2006d; 2011d), the researcher has established that 95% of counterfeit card fraud cases remained unsolved and that the perpetrators were never identified.

Furthermore, inspections showed that investigating officers have been unable to identify several pivotal aspects required to solve cases of counterfeit card fraud. These aspects include the point of compromise of the original card (i.e. the ATM or point of sale where the card had been skimmed and the card holder's personal identification number (PIN) obtained), the perpetrator who skimmed the card, the skimming device and PIN-capturing device used, the person(s) who manufactured and used the counterfeit card to commit fraud, the counterfeit card itself and the point of fraudulent spend (the ATM where the fraudulent cash withdrawal was made or merchant where the fraudulent purchase was made).

An examination of the training material used to train SAPS investigators in the investigation of counterfeit card fraud has confirmed the above mentioned challenges. Relevant SAPS training courses include the Basic Crime Investigation Course, Resolving of Crime Course and the Commercial Crime Forensic Learning Programme Levels I, II and III (SAPS, 2006g:67-71 & 89-101; 2009a; 2009b:64-66; 2009c:184-247; 2011c; 2012b). However, none of these courses address the investigation objective of identification in counterfeit card fraud cases. The researcher acknowledges the importance of this topic to be researched in order to enhance the understanding of investigating officers of the use of identification methods in the investigation of counterfeit card fraud.

1.3 RESEARCH AIM

The aim of a research project is the general intention or overall purpose of the research undertaken. It is a broad statement of what the research sets out to achieve and must be clear (Mouton, 2008:50-51). The aim of this study is to evaluate identification methods used to investigate counterfeit card fraud.

1.4 RESEARCH PURPOSE

The purpose of research is to provide answers to questions, to gain knowledge, to solve a practical problem or to improve existing procedures (Dantzker & Hunter, 2012:12; Denscombe, 2010:7; Badenhorst, 2007:23). Creswell (2009:111) underlines the importance of a clear, specific and concise purpose statement which will, from the outset, help to determine the focus and direction of the research, and provide an important criterion to evaluate the outcome of the research.

The purpose of this study includes the following:

- To explore the topic and the research problem which have been identified.
- To examine and evaluate identification methods used to investigate counterfeit card fraud.
- To empower investigating officers with knowledge on the use of identification methods in the investigation of counterfeit card fraud.

The researcher has gathered as much information as possible in respect of the problem relating to identification, which was found to be unsuccessful during counterfeit card fraud investigations, resulting in a high rate of unsolved cases. During the study, the prevailing situation in the South African Police Service and the banking industry has been examined to determine how counterfeit card fraud is investigated, whether identification is pursued during investigations and, if so, whether the identification methods used, are effective.

The researcher has examined and evaluated different identification methods that can be used to identify aspects specific to situations which an investigator may encounter in counterfeit card fraud cases. Furthermore, the study has been conducted to determine whether any good or effective practices exist in this regard and, if any, what they are and whether they can be used by investigating officers.

1.5 RESEARCH QUESTIONS

Good research begins with identifying a good question to ask, ideally a question that no one else has ever thought to ask before (Leedy & Ormrod, 2013:29). Research questions should elucidate exactly what is to be researched and deal with the specific issues that are to be researched, measured, observed and investigated

(Denscombe, 2002:31; Noak & Wincup, 2004:122). They are formulated to focus the study, and to give guidance in respect of a suitable research design and approach (Maxwell, 2005:67).

The research questions that have been researched in this study are:

- What are the objectives of forensic investigation in counterfeit card fraud investigations?
- What identification methods can be used to investigate counterfeit card fraud?

1.6 KEY THEORETICAL CONCEPTS

1.6.1 Forensic investigation

Forensic investigation is described by Benson, Jones and Horne (2015:2 & 19-20) as a process of inquiry into criminal conduct, a civil or administrative matter, which is an in-depth, meticulous search for the truth through the use of specialised skills, expert knowledge, and scientific methods and techniques (also see Van Rooyen, 2008:7, 14 & 77).

1.6.2 Evidence

Evidence is anything that is relevant to a case that can be used to prove or refute (disprove) a fact or allegation. It is anything with evidential (probative) or exculpatory value and includes, but is not limited to physical objects, documents, information and witness testimony (Dutelle, 2011:3; Gardner, 2012:7).

1.6.3 Fraud

Fraud is the unlawful, intentional making of a misrepresentation with the intent to defraud, causing actual or potential prejudice to another (Snyman, 2006:523; Burchell, 2005:833). The elements required to prove fraud are unlawfulness, intent, the making of a misrepresentation, the intent to defraud and a resulting actual or potential prejudice to another party.

1.6.4 Identification

Identification is the classification process by which an entity, person or object is placed in a predefined class or category, based on shared or similar features or

characteristics (i.e. class characteristics) (Osterburg & Ward, 2010:36). This forms the basis for individualisation, which relates to a unique (positive) identification (Van Graan & Budhram, 2015:47 & 64).

1.6.5 Individualisation

Individualisation is the process by which it is unequivocally established that physical evidence originates from a singular source or origin, exclusive of all others. This includes "… the demonstration that a particular sample is unique even among members of the same class" (Kaye, 2009:15; Marais, 1992:20-22).

1.6.6 Debit card

PASA (2012b:1) defines a debit card as a payment instrument issued by a financial institution and linked to a deposit account (such as a cheque, savings or transmission account) which, generally, is pre-funded and has a lower credit risk exposure than a credit card.

1.6.7 Credit card

A credit card is a payment instrument issued by a financial institution and linked to a credit card account with a pre-approved credit limit, which enables the cardholder to purchase goods and services from merchants who have agreed to accept the card (PASA, 2012b:1).

1.6.8 Card skimming

Card skimming involves the illegal copying of encoded information (data) from the magnetic strip of a legitimate card, making use of an electronic card reader (skimming device) with the intention of using the copied data for encoding and producing a counterfeit card for purposes of fraudulent transactions (Sabric, 2012:30; 2014:19).

1.6.9 Counterfeit card fraud

Counterfeit card fraud entails fraud arising from the use of an illegally manufactured bank card using data that has been copied (skimmed) illegally from the magnetic strip of a genuinely bank-issued card (Sabric, 2012:28; 2014:18). Counterfeit card fraud requires the skimming of card data from a genuine bank card, obtaining the personal identification number linked to the card, encoding another card (i.e. the

counterfeit card) with the skimmed card data, and transacting with the counterfeit card using the cardholder's PIN.

1.6.10 Method

The Oxford Dictionary (2014) describes a method as a particular systematic, orderly, planned or established procedure or process to accomplish or approach something, or to achieve a goal or objective.

1.7 VALUE OF THE RESEARCH

The aim of this research has been to evaluate the use of identification methods to investigate counterfeit card fraud. The research may provide investigators with an understanding of the effective use of appropriate identification methods in the investigation of counterfeit card fraud. Research should be worthwhile, address specific, current practical needs and should contribute to the development of existing knowledge (Denscombe, 2002:43-44). The researcher believes that the outcome of this study will be of value in different spheres.

Society, and more specifically cardholders, the banking industry and the business sector, will benefit from reduced levels in counterfeit card fraud. Counterfeit card fraud has a significant impact on the economy and finding solutions to prevent it or mitigate its impact will benefit everybody. An improved understanding of effective identification methods which can be used in counterfeit card fraud investigations may assist to increase the number of perpetrators who are identified positively. This should result in a higher detection rate and help to prevent the crime.

The South African Police Service will benefit from the new knowledge that has been created in respect of the research problem. This could assist to improve and enhance current SAPS training curricula, to ensure that investigators are more knowledgeable and better equipped to investigate and combat counterfeit card fraud through the use of effective identification methods. From an academic perspective, the research can serve as a basis for further research and developing best practices on how to use identification methods to investigate counterfeit card fraud effectively. The intellectual stimulus proffered by this research, could develop into appropriate strategies to combat counterfeit card fraud more effectively and may inspire academic researchers to undertake further research on the topic. The outcome of

this study can also be used by the academic community as a guideline and source of reference for future research.

1.8 RESEARCH DESIGN AND APPROACH

Research involves a scientific investigation into a specific phenomenon (Dantzker & Hunter, 2012:9). A research design is a plan or strategy that includes the underlying philosophical assumptions, specific selection of participants, data collection and data analysis techniques that will be used (Maree, 2012:70). Maxwell (2005:36) and Creswell (2009:5) state that the researcher's paradigm (worldview) will dictate the research design and approach. This research has followed a pragmatic worldview, where a research problem has been identified from reality and contextualised, focusing on the research problem and using all approaches available to understand the problem (Creswell, 2009:10).

The study is empirical in nature and is based on a qualitative research design, as explained by Welman, Kruger and Mitchell (2012:8-9) (also see Creswell, 2009:4 & 175). Empirical studies generate data from observation and experience (Maxfield & Babbie, 2012:5). A qualitative research design is intended to explore and understand the perception, interpretation and understanding of persons of a social or human problem or phenomenon. It deals with subjective data which is produced in the minds of participants.

A qualitative research process involves research questions that need to be answered, inductive data analysis and the researcher making interpretations of the meaning of data. It uses a wide array of data sources, including documents, records, observations, interviews and case studies. A qualitative research design has best suited the aim and purpose of this study, which required the collection of in-depth information in order to explore and understand the knowledge, interpretation, experiences and perceptions of counterfeit card fraud investigators and persons knowledgeable on the topic and research problem.

Data was collected from multiple sources, including relevant SAPS and Sabric records, participant interviews, national and international literature, and persons knowledgeable in the field of counterfeit card fraud. Data was collected from participants through semi-structured interviews, using an interview schedule.

Interviews with participants were conducted at their offices, and SAPS case files (dockets) were studied and analysed at the relevant police stations.

1.9 TARGET POPULATION AND SAMPLING

A population is the entire group or class of potential participants from which information is to be gathered (Dantzker & Hunter, 2012:198). The target population is the entire collection of units of analysis on which the research problem has bearing, while a sample is a group chosen from within the target population to provide the information required (Welman et al, 2012:52-53; Easton & McColl, [sa]: 1). Sampling is done when a population is large and it is impractical or uneconomical to study all the members of a population. A representative subset (i.e. sample) of the population is selected, making it realistic and feasible to study the participants included in the sample (Welman et al, 2012:55).

The target population for this study would include all SAPS and bank investigators investigating counterfeit card fraud. However, it was not possible to include all of them, because it would take a significant amount of time and resources to interview them all, and it would also be unrealistic and impractical. Therefore, a suitable sample had to be drawn. When selecting the sample, the researcher took into account the aspect of transferability of the research findings. This aspect is important during sampling and relates to the imaginative application of findings to other similar settings (Denscombe, 2002:150).

The research problem which the researcher set out to study was identified during docket inspections at the Commercial Crime Unit, Johannesburg. It was established from the unit commander that the unit functioned in different groups relating to different types of crimes investigated by the unit. A name list of all the investigators at the unit (which was divided into six groups) was obtained. By April 2013 there were 64 investigators working at the unit. Counterfeit card fraud cases were investigated by a specific group, namely the Banking Group (Group 3), which consisted of 15 investigating officers. The other groups did not investigate counterfeit card fraud and did not have the same practical experience or exposure to counterfeit card fraud cases. Investigators from the Banking Group were the most knowledgeable on the subject of counterfeit card fraud. For this reason, it was decided to include only the Banking Group in the study. Taking into consideration the

size of this group, it was decided to interview all 15 investigators and not to draw a sample from the group.

A sample which consisted of bank card fraud investigators was then selected, using the simple random sampling technique. The sampling was done for each bank independently, using its population of card fraud investigators, because they were the most knowledgeable on the topic of counterfeit card fraud and were exposed to counterfeit card fraud investigations on a daily basis. With simple random sampling, each member of the population has the same chance of being included in the sample (Welman et al, 2012:59). Firstly a name list of bank investigators who investigate counterfeit card fraud cases in Gauteng province was obtained from each of the following banks (the number of investigators is given in brackets): ABSA (9), Standard Bank (7), First National Bank (7), Nedbank (6), Capitec Bank (3), Postbank (3) and Ubank (3). The bank card fraud investigators totalled 38.

In determining the sample size of participants for interviewing, the researcher considered the five factors as discussed by Baker and Edwards (2012:18-19), namely data saturation, the minimum requirement for sample size, the style or theoretical underpinnings of the study, the heterogeneity of the population, and the breadth and scope of the research questions. After considering these, as well as the guideline of 20 to 30 participants suggested by Bryman (2012:425) and Creswell (1998) (as cited in Mason, 2010:3), a total of 27 card fraud investigators was considered to be adequate for the study.

For each bank, the names of the relevant card fraud investigators were recorded on pieces of paper of the same size, placed in a bowl and shuffled. A piece of paper was then drawn blindly. The remaining pieces of paper in the bowl were shuffled again and the process was repeated. The number of card fraud investigators for each bank, were drawn as follows: ABSA (3), Standard Bank (2), First National Bank (2), Nedbank (2), Capitec Bank (1), Postbank (1) and Ubank (1), totalling 12. The number of investigators drawn for each bank varied in accordance with the relative size of the bank's population of card fraud investigators compared to the other banks. A total of 27 card fraud investigators were selected for the study (15 from the SAPS and 12 from the banking industry).

In addition, two experts from Sabric were selected purposively, based on their applicable knowledge, experience, expertise and exposure to the field of counterfeit card fraud. Maxwell (2005:88) describes purposive sampling as choosing or selecting a particular group of participants in a particular setting with a particular purpose in mind, in order to obtain information that cannot be obtained from other participants equally well. It is important to choose a setting that offers the best opportunities and will yield the best data to learn about the research subject (Boeije, 2010:34-35; Leedy & Ormrod, 2013:152).

Sabric was chosen purposely, because the organisation collects, processes and disseminates information related to banking risks to the banking industry and relevant role players. It provides the industry with a national perspective of banking-related crime threats and trends, and facilitates a partnership approach to, inter alia, combat card fraud in cooperation with banks, merchants, the SAPS, the National Prosecuting Authority and other institutions (Sabric, 2013c:27). Sabric also provides investigative support to the SAPS and banks in respect of card fraud (SAPS, 2009d; 2010b; 2014) and is considered to be an important role player in the fight against counterfeit card fraud. Interviews were conducted with two senior officials from the Sabric Commercial Crime Office. Based on their extensive knowledge, expertise and experience in the field of counterfeit card fraud, they were able to provide a comprehensive, in-depth perspective on the topic.

1.10 DATA COLLECTION

Data is any form or representation of information, meaning or knowledge which may have meaning or informative value (Maxwell, 2005:79). In qualitative research, data can include virtually anything that the researcher sees, hears or that is otherwise communicated or relayed to the researcher, bearing in mind the constraints of applicable ethical principles. Data collection methods in qualitative research include observation, surveys, interviews, documents and focus groups (Maree, 2012:82-92; Dantzker & Hunter, 2012:200; Bouma & Ling, 2010:172-180). The following data sources and data collection methods were used during this study:

1.10.1 Literature

A review of literature resources in respect of the research topic and research problem is very important. A literature review puts the research in context within the

existing body of knowledge in the field that is being investigated (Denscombe, 2002:50). Welman et al (2012:38) emphasise the importance of a widespread review of literature in respect of the research problem and questions (also see Leedy & Ormrod, 2013:51).

The most effective way of reviewing existing literature is to generate keywords and search terms that are directly related to and describe the research problem, research questions and the purpose of the research (Creswell, 2009:29; Welman et al, 2012:40). This broadens the spectrum of literature resources with relevant data that could be used. Following this approach, various relevant keywords and terms were generated, based on discussions with colleagues and persons knowledgeable on the subject, including SAPS and bank counterfeit card fraud investigators and Sabric representatives. Keywords and search terms were also generated by consulting librarians from Unisa about the topic and the research problem, studying dictionaries, reading books on the subject and from the researcher's own experience in the field.

Keywords and terms generated for this study were used in an extensive literature review. National and international sources on relevant topics were consulted, including criminal investigation, forensic investigation, counterfeit card fraud, card skimming and relevant legislation, enabling the researcher to collect as much information as possible in order to answer the research questions and address the research problem. Data was collected from subject-specific books, journals, the World Wide Web (WWW) (Internet), articles, previous research, the media, official SAPS sources and publications from relevant role players. Literature relating to research methods, designs and research methodology was also consulted extensively. Various search methods and aids were employed using keywords and search terms, including computerised library catalogue searches (e.g. Unisa Oasis), Unisa and SAPS librarians, physical searches for applicable literature in libraries, and Web-based search engines (Google, Yahoo, Search.com and Internet Explorer).

The following keywords and terms were used to ensure a thorough literature review:

ATM; ATM skimmer; ATM-mounted skimming device; ATM skimming; Automated teller machine; Bank card; Bank card skimming; Banking-related crime; Bezel; Card encoder; Card reader; Card skimming; Card slot; Card slot overlay; Card technology;

Chip-and-pin card; Commercial crime; Common point of fraudulent spend; Common point of purchase; Counterfeit bank card; Counterfeit card; Counterfeit credit card; Counterfeit debit card; Counterfeit card fraud; Counterfeit bank card fraud; Counterfeit payment card fraud; Counterfeit debit card fraud; Counterfeit credit card fraud; Credit card; Criminal investigation; Debit card; Encoder; Evidence; Forensic investigation; Fraud; Fraudulent purchase; Fraudulent spend; Fraudulent transaction; Fraudulent withdrawal; Handheld skimmer; Handheld skimming; Handheld skimming device; High-tech skimming; High-tech skimming device; Identification; Identification method; Individualisation; Keypad; Keypad overlay; Magnetic strip; Magnetic stripe; Micro-camera; Personal identification number; PIN; PIN capturing; Pinhole camera; PIN recording; Point of compromise; Point of fraudulent spend; Point of purchase; Point of sale; Point of sale skimming; Skimming; Skimming device; Smartcard.

1.10.2 Semi-structured interviews

Maree (2012:87) describes an interview as a two-way conversation in which the interviewer (researcher) asks the participant questions with the purpose of collecting data, and to learn about the ideas, beliefs, views, perceptions, opinions, understanding and behaviour of the participant. The aim of a qualitative interview is to see the world (and the research problem) through the eyes of the participant. Furthermore, to obtain rich descriptive data that will help the researcher understand the participant's construction of knowledge and social reality.

In a semi-structured interview the participant is required to answer a set of predetermined questions, which are pre-recorded on an interview schedule to guide the line of inquiry. In addition to the predetermined questions, this type of interview allows the interviewer to use probing and exploring questions in order to obtain explanations and clarification from the participant (Blandford, 2013:23-25; Sewell, [sa]: 1-6). Probing and exploring questions help the interviewer to develop the topic, and explore ideas and avenues to obtain as much information as possible from the participant (Maree, 2012:87-88). The researcher used open-ended questions during semi-structured interviews to obtain as much information as possible in respect of the research problem and research questions. Open-ended questions provide no structure for an answer and are intended to invite a more comprehensive in-depth answer to a question (Bouma & Ling, 2010:65-66).

The interview schedule which has been used to interview participants from Sabric differed from the one used to interview card fraud investigators. The reason for this is that, although the two officials are very knowledgeable on the topic of counterfeit card fraud, work together closely with investigators and provide them with investigative support, their own responsibilities do not include the investigation of counterfeit card fraud.

Before any participant was interviewed, the researcher obtained formal approval from the South African Police Service in terms of SAPS National Instruction 1 of 2006 (Research in the Service) to conduct the research and interview SAPS investigators for purposes of the study (SAPS, 2006f). Approval from the SAPS is attached hereto as Annexure A. The interview schedule used during interviews with SAPS and bank investigators is attached hereto as Annexure B. The interview schedule used to interview the participants from Sabric is attached as Annexure C.

Leedy and Ormrod (2013:154) provide a number of guidelines for interviewers to ensure effective and productive interviews, which were followed by the researcher. Prior to interviews, consent was obtained from each participant to be interviewed. Each participant was interviewed separately and in private. The researcher established and maintained rapport with the interviewee by introduction and explaining the background, purpose and scope of the interview. The researcher first asked a number of questions on the participant's background, interests and experience to allow the participant to get familiarised with the situation and invited the participant to speak freely and openly at all times. Participants were ensured of their privacy and the confidentiality of interviews, and encouraged to be open and forthcoming. Audio recordings were made of interviews, of which transcriptions were later made for analysis. Responses were also carefully recorded in writing and discussed with the participant afterwards to make sure that information had been captured correctly.

1.10.3 Personal experience

The researcher has 27 years' service in the South African Police Service, of which 25 years as an investigating officer, having spent the last 14 years of his career as a commercial crime investigator and commander in the Commercial Crime Unit. The researcher was responsible for, inter alia, the investigation of counterfeit card fraud

and other commercial related crime. In addition, the researcher regularly conducted docket inspections at different commercial crime investigation units.

The researcher was able to draw from extensive experience, training and exposure to the field of commercial crime and counterfeit card fraud investigations. Throughout the study this has added significant value to the data collection and analysis processes, the interpretation of data, the findings and recommendations. The background of the researcher has proven to be very useful when interviewing investigators, understanding and interpreting their responses, ideas and perceptions in context. The researcher has a thorough understanding of the banking crime environment and card fraud landscape, the subject-specific terminology and language used, as well as the contents of SAPS counterfeit card fraud dockets, relevant systems and records.

1.10.4 Case files

As part of the overall research design of the study, the researcher studied and analysed a sample of SAPS case dockets relating to counterfeit card fraud. This made it possible to establish how counterfeit card fraud cases were investigated in practice, as opposed to theory, ideal case situations and investigation methods which participants might describe during interviews. Case dockets, on the other hand, could also be used to corroborate the views and responses given by participants. This exercise provided useful insights into what happened in reality when these cases were investigated.

The researcher studied and analysed the contents of 100 selected counterfeit card fraud dockets that were registered on the Crime Administration System (CAS) of the SAPS between 1 December 2012 and 31 March 2013 at SAPS stations located in Johannesburg. Since it would have been impractical to study counterfeit card fraud dockets from all the stations in Johannesburg, a number of them were selected by using cluster sampling. Cluster sampling is done by dividing a population into small, non-overlapping groups (i.e. clusters) using a simple random sampling technique (Maree et al, 2012:175-176). Cluster sampling was also used to include diversity that might exist in counterfeit card fraud dockets investigated by different investigation units.

A name list of all SAPS stations located in Johannesburg was obtained from the website of the South African Police Service. Stations in Johannesburg were chosen because these were serviced by the Commercial Crime Unit, Johannesburg, where the research problem was identified. The list consisted of 46 SAPS stations, which were confirmed by the unit commander of Johannesburg CCU as being stations falling in their service area. The names of the 46 stations were recorded on even-sized pieces of paper and, using simple random sampling, a total of 15 stations were drawn.

A list of all fraud cases that were registered at the selected stations during the period selected was obtained from the system manager of CAS at the Division Technology Management Services (Information Systems Management) of the SAPS. CAS does not distinguish between counterfeit card fraud cases and other fraud types. A fraud case can be registered on CAS under any of nine fraud types, distinguished by nine different crime codes. However, none of these relate to counterfeit card fraud specifically.

There are two fraud crime codes relating to general fraud types on the system, namely codes: 61010(3400) and 64505(3506), but the possibility existed that counterfeit card fraud cases could have been registered under any of the nine fraud codes. Therefore, the researcher included all nine fraud codes in order to identify counterfeit card fraud cases. The researcher established whether the CCU Johannesburg or relevant station level investigation units had any counterfeit card fraud dockets on hand, which were registered during the selected period. However, neither the CCU nor any station level investigation unit had any of the dockets on hand. All counterfeit card fraud dockets registered during the selected period had already been finalised and archived.

The researcher then visited each of the 15 stations with its list of fraud dockets that had been registered during the selected period, and identified all the counterfeit card fraud dockets by perusing the contents of the fraud dockets. At each station the case numbers of counterfeit card fraud dockets were recorded on even-sized pieces of paper. Using a simple random sampling technique as described above, a sample of counterfeit card fraud dockets was selected for each station independently.

The 100 counterfeit card fraud dockets selected at the various stations consisted of the following samples, indicated as sample/number of registered counterfeit card fraud dockets (see pages 104 to 107): Booysens (3/5); Bramley (4/8); Brixton (2/6); Carletonville (15/42); Douglasdale (9/23); Hillbrow (11/28); Jeppe (4/8); Johannesburg Central (13/36); Linden (3/9); Norwood (4/11); Randburg (6/14); Rosebank (4/9); Sandton (9/24); Westonaria (6/15) and Yeoville (7/9). The total number of registered counterfeit card fraud dockets for the 15 stations for the selected period was 247. The sample size drawn for each station varied in accordance with the size of the study population for each station relative to the entire study population of 247 dockets.

Dockets were studied and analysed, not only to compare actual recorded counterfeit card fraud investigations with information collected during interviews, but also for the following reasons:

- To establish whether identification methods were used to investigate the cases.
- To establish what identification methods were used (if any).
- To evaluate how effective the identification methods (if any) were in achieving a positive identification of the perpetrator(s).

Data obtained during the docket content analysis was compared with information that was obtained during interviews from SAPS investigators. The docket analysis formed part of the study for which prior approval was obtained from the SAPS (see Annexure A as per attached). Access to the case files of banks relating to counterfeit card fraud investigations could not be obtained. Bank investigators indicated that their case files were confidential and could not be made available for the study.

1.10.5 Official records and documents

Official statistics relating to counterfeit card fraud reported to the South African Police Service were obtained from annual reports of the SAPS. Other official records, which were of importance for the study, included records from the Crime Administration System relating to fraud cases (see paragraph 1.10.4) and selected case dockets.

The Geographic Information System (GIS) of the SAPS was used to conduct crime pattern analyses and generate crime maps specifically relating to fraud (see paragraph 3.2.1.3 (a)). Relevant SAPS directives and policies, including the mandate of the CCU and the SAPS strategy and standard operating procedure in respect of counterfeit card fraud and card skimming cases, were also used as sources (SAPS, 2009d; 2010a). Furthermore, the researcher studied a number of official SAPS reports relating to counterfeit card fraud cases, which were reported between 2010 and 2014 in which the perpetrator(s) was/were identified positively either before or during the investigation phase (see Annexure F for a summary). Access to these reports was obtained with prior consent from the SAPS (see Annexure A as per attached).

1.11 METHOD OF DATA ANALYSIS

Data analysis is a process of inspecting, cleaning, transforming and categorising or modelling data with the goal of interpreting and understanding it, as well as identifying patterns, critical events and irregularities, describing events and highlighting useful information (Taroni, Bozza, Biedermann, Garbolino & Aitken, 2010:4; Levine, 1996:1).

The researcher followed four primary steps to analyse data, as proposed by Creswell (2007) in Leedy and Ormrod (2013:158-159), as follows:

- Organisation

Data was organised using index cards, folders and Microsoft Excel spreadsheets. Data was broken into smaller units (paragraphs, sentences and words). Different categories were created and hard copy folders, computer folders and separate spreadsheets were opened for each. The categories related to relevant themes and key concepts, namely forensic investigation, the objectives of forensic investigation, counterfeit card fraud, counterfeit card fraud modus operandi (method of operating) (see paragraph 3.2.1.5), card skimming, counterfeit card fraud devices and equipment, and identification methods used to investigate counterfeit card fraud. The latter was divided into several sub-categories relating to, inter alia, methods to identify the point of compromise (skimming and PIN capturing) of a bank card, the point of fraudulent spend (fraudulent withdrawal or purchase using the counterfeit

card) and the perpetrators involved in the different stages of the crime. In practice a source often produced information in respect of more than one data category. The applicable information was then recorded under the appropriate categories, referenced with the source and cross-referenced with each other.

- Perusal

All sources of data were perused several times to get an overall sense (overview) of what the information as a collective entailed. Transcripts of individual interviews, relevant literature, official records and the content analysis of SAPS case dockets were perused thoroughly and in depth after categorisation. This was also done with the researcher's own research notes and comments made during the course of the study.

- Classification

The researcher identified subcategories, themes and subthemes, and classified them using a system of coding. Coding is a process where a numerical, alphabetical or alpha-numerical code is assigned to each keyword or key concept (Welman et al, 2012:213). Coding was done inductively from data collected, as proposed by Given (2008:85-88). For example, a card skimming modus operandi using a false keypad overlay for PIN capturing was coded as KO under the subtheme 'PIN-capturing methods' (PINCAP), under the theme 'modus operandi' (MO), which resorted under the category 'card skimming' (CARDSK). Coding is essentially labelling or tagging concepts, keywords and meanings that are identified from data. The researcher used IBM i2 Analyst's Notebook software to compile a free association chart depicting a 'relationship tree' illustrating the parent-sibling relationships and links between categories, subcategories, classes, themes, subthemes, groups and subgroups of data. This helped to create a better understanding of relationships between concepts and themes in the study.

- Synthesis

The frequency of concepts and keywords was determined, using the sorting function of a Microsoft Excel spreadsheet and analysis functions of Analyst's Notebook. Appropriate indexes, tables, matrices, diagrams and visual representations were

generated, depicting the overall results of the data analysis process. The different sources were integrated at this stage. For example, interview transcripts that referred to specific issues and concepts, which also appear in previous research, an Internet source or a text book were cross-referenced and summarised together.

1.12 METHODS TO ENSURE TRUSTWORTHINESS

In order to ensure rigour and trustworthiness in qualitative research, specific strategies should be followed to meet five criteria, being credibility, transferability, dependability, confirmability and authenticity (Gray, 2014:185-186). The researcher applied various strategies to meet these criteria, as proposed by Savin-Baden and Major (2013:476-480), Shenton (2004:63-75) and Creswell (2013:249-253).

1.12.1 Credibility

Credibility is the extent to which a test or measuring instrument measures what it intends or claims to measure (i.e. the effectiveness, applicability and appropriateness of the data collection instrument). Strategies to ensure credibility include prolonged engagement, time spent in the field and persistent observation, triangulation, random sampling, peer review/debriefing, negative case analysis, clarifying researcher bias, member checking and using a rich, thick description for observations.

The researcher's career spans 14 years as a commercial crime investigator, during which extensive knowledge and experience in respect of counterfeit card fraud investigations were acquired. This background knowledge was used to validate data which was collected during the study. The study was done over a period of three years, which afforded sufficient opportunity to engage in the field of counterfeit card fraud investigations and collect an adequate amount of information in respect of the research topic.

During the study, triangulation was used to validate data from different sources. Information obtained from different sources was compared in order to verify its correctness and accuracy. Triangulation involves the use of multiple and different sources, methods, researchers and investigation strategies to corroborate evidence and findings (Creswell, 2013:251; Golafshani, 2003:603). The researcher used various sources to do this, including information collected from participants during

interviews, data obtained from subject-specific textbooks and literature, official reports and SAPS case dockets relating to counterfeit card fraud. Peer review was also applied by discussing the research process, data collection and analysis, and findings of the study with independent knowledgeable colleagues who did not form part of the group of participants. Their perspectives and ideas were also used to corroborate those of the participants.

The researcher's past experiences, biases, prejudices and assumptions should be stated from the outset in order to provide an understanding of the researcher's position, approach and interpretations (Noble & Smith, 2015:34-35). There was no specific bias, prejudice or assumption relating to the research topic or research questions that could influence the approach, interpretations or findings of the researcher. The topic was approached in an objective manner, working with facts and information from the researcher's working environment as a commercial crime investigator, and the perspectives of participants. Member-checking was also used to ensure credibility of the findings of the study. Participants were provided with interview transcripts and the findings of the study, and feedback was obtained in respect of the accuracy and credibility thereof.

1.12.2 Transferability

Transferability relates to the extent to which the findings of a study can be applied to other situations (Shenton, 2004:69). A strategy to meet the requirement of transferability involves the use of such a detailed, abundant, in-depth description of themes, contextual factors impacting on the study, participants' views and observations, that it enables readers to transfer the information provided by the researcher to other settings and circumstances. The researcher must also clearly state any restrictions or inhibiting factors which have impacted on the study.

The reader himself/herself must be able to determine the degree to which the findings of the study can be transferred and considered as relevant to other settings and circumstances. Throughout the study, the researcher placed emphasis on recording and describing data and observations using a rich, thick (dense) descriptive language, abundant in detail, description and meaning to ensure that the study would be transferable to the larger counterfeit card fraud environment.

In addition, Gray (2014:185) proposes the use of purposive sampling as a strategy to ensure transferability through pertinent and similar contextual factors. This was done by selecting and interviewing two specific knowledgeable participants from Sabric.

1.12.3 Dependability

Dependability concerns the stability and consistency over a period of time of the research design, data collection methods and instruments to produce consistent results under the same circumstances and in the same context (Dantzker & Hunter, 2012:188; Bouma & Ling, 2010:83). Gray (2014:185) suggests the use of clear audit trails throughout the data to ensure dependability, while Shenton (2004:71) posits a thorough description by the researcher of the research design and all processes and methods used during the study to enable future replications of the study.

A detailed description of the research design, data collection and data analysis methods was provided, including the sampling procedures which were followed. The researcher made use of standard interview schedules to guide interviews with selected card fraud investigators and Sabric participants. Interviews were recorded and participants' responses captured verbatim in writing. Furthermore, a detailed reference list of all sources used was compiled and sources were properly cited.

1.12.4 Confirmability

Confirmability involves objectivity in the study. Researcher bias should be neutralised by using strategies such as triangulation and clarifying preferences the researcher might have had. A detailed audit trail of the research process, data collected, data analysis and the researcher's interpretations and conclusions is critical to meet the requirement of confirmability (Shenton, 2004:72; Given, 2008:43-44). In order to achieve this, the researcher used triangulation as a strategy, kept a research diary and maintained a proper audit trail of the entire research process.

1.12.5 Authenticity

Authenticity relates to the reassurance that the constructs and evaluation of research are genuine and credible, both in terms of the real-life experiences and perceptions of participants, and within the wider social and political context in which it is undertaken (Given, 2008:44). A study is authentic when it is fair towards participants, reflects the true viewpoints and ideas of participants, and endeavours to action

participants to cooperate in improving their social reality. Hence, authenticity is achieved by promoting fairness to participants, ontological authenticity (an understanding of the viewpoints and ideas of others), educative authenticity (the education of participants), catalytic authenticity (stimulating and actioning participants) and tactical authenticity (empowering participants to act).

Gray (2014:186) and Morrow (2005:252-253) point out that data can be interpreted differently and that different explanations and conclusions are possible from the same set of data. The researcher must be aware that data can lead to contradicting findings, realities and conclusions, and also report these.

The researcher used the study to educate and empower participants with knowledge on the topic of the use of identification methods in counterfeit card fraud investigations. A proper audit trail of the entire research process was kept to support the trustworthiness and authenticity of the study. The researcher also ensured that participants were treated fairly and that interpretations, inferences and conclusions made were rational and substantiated by actual data collected.

1.13 ETHICAL CONSIDERATIONS

Ethics in research relates to doing what is morally and legally right when conducting research (Grix, 2010:143; Dantzker & Hunter, 2012:190). Throughout the study, the researcher maintained the highest ethical standards, as discussed by Leedy and Ormrod (2013:104-109), namely:

- *Protection from harm*: No harm of a physical, psychological, social or emotional nature was caused to any participant. No stress, embarrassment or loss of self-esteem was caused during the research.
- *Right to privacy and confidentiality*: No person's right to privacy or confidentiality was violated. The researcher treated the identities and responses of participants as strictly confidential. These have not and will not be revealed to anyone, unless written consent is given by a participant.
- *Voluntary, informed participation and obtaining prior consent*: The researcher made sure that participation in the study was completely voluntary. Participants were informed prior to participation what the purpose of the study and the interview was, and what it entailed. Informed

written consent was obtained from each participant prior to any participation.

- *Consent to conduct research in the SAPS*: Prior written consent was obtained by the researcher to gain access to and study official SAPS records, to conduct research in the SAPS in terms of its research policy and to interview SAPS investigators.
- *Honesty with professional colleagues*: Findings were reported in a complete and honest manner without any misrepresentation. No data or findings were inflated, falsified or fabricated.
- *Maintain high standards, avoid plagiarism and acknowledge sources*: The researcher strived towards maintaining high standards of research throughout the study. He avoided plagiarism at all times and did not intrude on anyone's intellectual property rights. Where data was unavailable or any aspect required further research, it was stated clearly. All sources were properly referenced, and the work of other authors was properly cited and acknowledged.
- *Professional codes of ethics*: The researcher adhered to the Unisa Policy on Research Ethics, and applicable institutional policies and guidelines at all times (University of South Africa, 2012). Data collected during the research will be kept for a period of at least five years. The researcher is aware that copyright of the data collected and the research report belongs to the University of South Africa.

CHAPTER TWO:
FORENSIC INVESTIGATION IN COUNTERFEIT CARD FRAUD CASES

2.1 INTRODUCTION

The application of scientific knowledge in criminal investigations has led to an inevitable symbiosis of the two, giving rise to the now widely recognised discipline of forensic investigation. Today, the thought of criminal investigation without the support of forensic science is largely unthinkable (Monckton-Smith, Adams, Hart & Webb, 2013:24-25). As scientific knowledge grew, so did its application in the field of investigation.

The origin of forensic pathology can be traced as far back as 1250 when a book on post-mortem examinations was published in China (Becker & Dutelle, 2013:6-8). Coroners charged with determining the cause of death of a person existed in England by 1272. Early scientific advances included the anthropometry of Alphonse Bertillon in 1883 and a fingerprint classification system by Sir Francis Galton in 1892. Hans Gross, an Austrian prosecutor and judge, published a text in 1893 in which he advocated the application of scientific disciplines to the field of criminal investigation (Dutelle, 2011:9). Developments like these paved the way for a modern scientific approach in criminal investigation and gradually led to modern forensic investigation methods.

Criminals who commit counterfeit card fraud have become very sophisticated and knowledgeable with regard to card skimming and card counterfeiting methods and technologies. If investigators want to investigate this crime successfully, they must not only be conversant with these methods and technologies, but stay a step ahead by applying forensic science effectively.

In this chapter, forensic investigation, its objectives and application to counterfeit card fraud are discussed, while the methods and equipment used to commit the crime are explained.

2.2 FORENSIC INVESTIGATION

Forensic investigation developed over many years in the field of criminal investigation. Criminal investigation can be described as a process of inquiry into a

criminal or unlawful act, which involves the identification, collection, preservation and evaluation of information and evidence (Van der Westhuizen, 1996:1-3; Dutelle, 2011:4 & 17; Benson et al, 2015:19). It is an in-depth search for the truth with the main purpose of finding a solution to a crime by finding evidence that will prove who committed the crime, bringing the identified perpetrator before court, preparing a case for criminal prosecution and assisting to ensure a successful prosecution. The investigation process includes searching, reasoning, examination and analysis, which is conducted in a thorough, systematic, organised and thoughtful manner.

Evidence gathered during criminal investigations is often supported and supplemented by scientific knowledge and evidence of a scientific nature, which are derived from a forensic science discipline, hence the application of forensic investigation to investigate crime (Monckton-Smith et al, 2013:23-25). The term 'forensic' means characteristic of or suitable for a court of law (Nickell & Fischer, 1999:1). Forensic investigation is a process of inquiry into criminal conduct, a civil or administrative matter, which is an in-depth, meticulous search for the truth through the use of specialised skills, expert knowledge, and scientific methods and techniques (Van Rooyen, 2008:7, 14 & 77-78; Benson et al, 2015:2 & 19-20).

A key element of forensic investigation is the application of forensic science to enhance and support evidence. It is not only applicable to the investigation of crime but also applies in civil and administrative matters and questions arising from litigation. Van Rooyen (2008:78) argues that police investigators who investigate crime in a court-directed manner, while applying scientific knowledge and principles, should be seen as forensic investigators.

Forensic science is the application of scientific knowledge and principles to legal disputes, whether criminal or civil (Chisum & Turvey, 2011:4-5). It includes different scientific disciplines, among which forensic medicine, ballistics, pathology, toxicology, serology, biology, psychology, psychiatry, dactyloscopy, forensic document examination, digital forensic examination and forensic tool mark examination. Becker (2009:12) and Dutelle (2011:6) emphasize the importance of applying forensic science to physical evidence in order to increase and enhance its evidential value. The forensic expert knows how to extract the meaning of physical evidence, while the investigator knows how to put its meaning into context.

During interviews, investigators were asked what forensic investigation is. Some included more than one key theme in their responses. A breakdown of the responses is as follows:

- It involves the application of forensic science to solve crime (22 participants).
- It involves scientific methods used on crime scenes to detect forensic clues during crime scene investigations (18 participants).
- It means investigating for purposes of the court (17 participants).
- It is done by scientific experts in a forensic science laboratory and involves analysing exhibits in a laboratory (9 participants).
- It involves auditing, accounting and financial transactions/ financial crimes (4 participants).

The responses showed that, although participants differed to an extent, the majority understood forensic investigation in their environment as the application of forensic science to criminal investigations with the aim of presenting evidence in a court of law.

2.3 RESPONSIBILITY, MANDATE AND POWERS TO INVESTIGATE

In South Africa, investigators can be divided into two broad categories, namely SAPS investigators and non-SAPS investigators. Non-SAPS investigators include government departments and agencies, as well as private entities with investigative capacity (Benson et al, 2015:14-18). Different statutes confer powers of investigation on a number of institutions and persons. The extent and purpose of these powers vary, and can include one or more functions such as criminal investigation, questioning, inspecting, obtaining records and information, search and seizure, summoning, arrest, collecting evidence and hearing testimony.

2.3.1 South African Police Service

The SAPS is the primary crime investigation body in South Africa. Section 205(3) of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) places a legal obligation on the South African Police Service to, inter alia, investigate crime. In addition, the legal framework for the investigation of crime by the SAPS is established by the South African Police Service Act, 1995 (Act No. 68 of 1995), the

Criminal Procedure Act, 1977 (Act No. 51 of 1977) (CPA) and different statutes which declare certain types of conduct as offences. The mandate for the investigation of counterfeit card fraud jointly rests with the Commercial Crime Unit of the DPCI and station level detectives of the SAPS (see paragraph 1.2).

2.3.2 Non-SAPS investigating institutions and persons

2.3.2.1 Government-related institutions and agencies

Non-SAPS government-related institutions and agencies which have powers to investigate, include the Special Investigating Unit, the National Prosecuting Authority, the Public Protector, registered auditors, the South African Revenue Service, Military Police, Independent Police Investigative Directorate, Customs and Excise, and others. In terms of the Customs and Excise Act, 1964 (Act No. 91 of 1964) customs officials can make arrests, search persons, premises, packages and containers. They can also detain prohibited and illicit goods, which include skimming devices and equipment intended for card skimming and/or card counterfeiting.

2.3.2.2 Bank, corporate and private investigators

Certain banks, companies and corporations have internal ('in-house') investigators who conduct investigations in the course and scope of their normal business to safeguard their security, strategic, operational or business interests (Benson et al, 2015:17-18). Investigations include employee misconduct, security breaches, loss and theft of assets, and offences specifically targeting the clients and/or systems, instruments, resources or products of the bank or business (Van Rooyen, 2008:59).

The Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001) in section 1 distinguishes between private investigators and internal investigators. In terms of the Act, a private investigator is a person who, in a private capacity and for the benefit of a third party, investigates the identity, actions, character, background or property of another person without his/her consent. Private investigators need to register with the Private Security Industry Regulatory Authority (PSIRA). Internal investigators do not have to register with PSIRA.

Although internal bank and corporate investigators act on behalf of their employers, evidence collected during internal investigations is recognised and accepted by

South African courts[1]. Evidence obtained during private investigations is also accepted by South African courts[2].

During interviews, all the bank investigators described their functions and responsibilities as the investigation and combating of card-related fraud, including counterfeit card fraud, and protecting the interests of the bank and its clients. SAPS investigators are better equipped to investigate counterfeit card fraud through cooperation with bank investigators and the South African Banking Risk Information Centre. The reason being that they can provide SAPS investigators with information and intelligence in respect of banking-related crimes, including identified points of card skimming and PIN capturing, and points of fraudulent spend in counterfeit card fraud cases.

Furthermore, bank investigators can provide court-directed evidence to SAPS investigators, including the particulars of account holders and copies of bank records (for example, account opening documents and account statements) in terms of sections 205 and 236 of the Criminal Procedure Act, 1977 (Van Niekerk, Lochner, Naidoo & Zinn, 2015:233-234). Bank investigators have the power to arrest under certain circumstances. In terms of section 42(1)(a) of the Criminal Procedure Act, 1977 a private person may, without a warrant, arrest anyone who commits or attempts to commit in his/her presence, or is reasonably suspected of having committed an offence listed in Schedule 1 to the Act. This includes fraud, theft, forgery and uttering. Therefore, a bank investigator may without a warrant, on the basis of evidence gathered during his/her own investigation, which provides reasonable grounds to suspect a person of committing any of the crimes mentioned, arrest the suspect and hand him/her over to the police.

2.4 THE PURPOSE AND OBJECTIVES OF FORENSIC INVESTIGATION

The purpose of forensic investigation is to investigate evidence in a scientific manner and to determine how evidence can be used to prosecute an offender or, said

[1] In *S v Dube* 2000 1 SACR 53 (N) the court accepted the evidence of an investigator who conducted an internal investigation into thefts that were taking place at a motorcar manufacturer. The evidence related to photograph and tape recordings made by the investigator, acting as an agent of the employer during an undercover trap.

[2] In *Lachman v The State* (432/09) [2010] ZASCA 14 the Supreme Court of Appeals admitted testimony relating to a search which was conducted by a police official assisted by a private investigator.

differently, to identify, collect and present all relevant evidence to enable a court of law or other presiding authority to establish the truth in respect of an alleged crime or issue under dispute (Benson et al, 2015:11-13). An investigation can be compared to a project, which has a predetermined goal and specific objectives aimed at achieving it. Objectives are specific deliverables or outcomes and provide clear, measurable milestones which the investigator must achieve.

During interviews, investigators were asked what the purpose of forensic investigation is. The majority of participants (22) included in their responses the identification, tracing and charging of the suspect, collecting relevant evidence in the case, and making use of science and scientific methods to improve evidential value and the interpretation of evidence in order to prove the case. Five (5) participants viewed the purpose of forensic investigation only as the application of forensic science to improve evidential value during criminal investigations. One (1) participant also stated that an additional purpose is to determine the root causes and motives for committing crime, which will contribute towards managing future crime by addressing the root causes and implementing suitable preventive measures.

Investigators were also asked what the purpose of forensic investigation is in counterfeit card fraud cases. The following is the result of the most prevalent responses received (certain participants provided more than one concept in their responses). The purpose of forensic investigation is to:

- Identify the merchant(s) and/or ATM(s) where the fraudulent spend (negative spend) took place (24 participants).
- Identify all persons involved in the commission of the crime, including the person responsible for skimming the card, the manufacturer of the counterfeit card and the person (runner) who withdraws money or makes purchases with the counterfeit card (23 participants).
- Identify the merchant or ATM where the card was skimmed and PIN captured (22 participants).
- Collect all relevant evidence and obtain statements from all witnesses (22 participants).

Although the responses from participants illustrated a general understanding of the purpose of forensic investigation and in particular in counterfeit card fraud cases, responses also included a number of objectives of forensic investigation. Various authors agree on the objectives of investigation (Orthmann & Hess, 2013:11; Becker, 2009:11-12; Swanson, Chamelin & Territo, 2003:28), which include:

- Identification of the crime.
- Identification of the perpetrator(s).
- Individualisation of the crime.
- The collecting and processing of evidence and information.
- The evaluation of evidence and information.
- Tracing the suspect(s) and ensuring court appearances.
- Recovery of property and restitution.
- Support and involvement during the prosecution/litigation phase.
- Victim empowerment.

Stelfox (2013:2-3) argues that, in addition to the above, criminal investigation also has other objectives, including community reassurance, intelligence gathering, disruption of criminal networks and managing crime risks (also see Benson et al, 2015:13; Karagiozis & Sgaglio, 2005:112-122). In the private sector and other spheres outside the SAPS, the purpose and objectives of forensic investigation are not restricted to the investigation of crime, as investigation mandates may differ from that of the SAPS. Bank, corporate and private investigators conduct investigations to protect the interests of their clients or employers. Therefore, the scope and focus of their investigations may not necessarily include the investigation of crime (Benson et al, 2015:10-12 & 24-25).

The following discussion deals specifically with the objectives of identification and individualisation in counterfeit card fraud investigations, as these two objectives have direct bearing on the research problem and research questions.

2.4.1 Identification

Identification is the classification process by which an entity, person or object is placed in a predefined class or category, based on shared or similar features or characteristics (i.e. class characteristics) (Osterburg & Ward, 2010:36; Fisher,

2004:5; Champod, 2015:95). During interviews, all the participants were able to provide a general explanation of the concept of identification. It was established from summarised responses of participants, official SAPS reports (see Annexure F as per attached), SAPS directives (SAPS, 2010b:1-3; 2011a; 2011b:1-16) and case dockets analysed that various aspects related to incidents of counterfeit card fraud need to be identified during investigation. These include the following (see paragraph 3.2.1 for a detailed discussion):

- The crime scene(s) (i.e. the scene where the original bank card was skimmed and the cardholder's PIN captured, and the scene(s) where the fraudulent transaction(s) took place, namely an ATM or point of sale at a merchant).
- The victim(s) (often a fraudster is responsible for skimming and counterfeiting multiple cardholders' cards).
- The suspect(s) (including the person who skimmed the original card(s) and obtained the PIN(s), the person responsible for producing the counterfeit card(s) and the person(s) responsible for the fraudulent transaction(s)).
- Witnesses (including the victim, eyewitnesses, police officials, bank officials and the digital forensic expert).
- Equipment used (all relevant equipment involved, including the skimming device, PIN-capturing device, card encoder, computer equipment and the counterfeit card(s)).

In reality, counterfeit card fraud manifests in different case settings (see Annexure F and the list of SAPS dockets analysed). The circumstances and settings of cases often differ when a case is reported for investigation. In certain cases the identity of one or more aspects may already be known at the start of the investigation (e.g. the victim may be known, a suspect may already be in custody, the crime scene may be known and/or a skimming device may have been seized). Therefore, the aspects which need to be identified may differ from case to case and will depend on the specific circumstances of a case.

Identification needs to be followed by a process of individualisation, during which the unique (positive/definite) identity of the suspect is established by means of relevant evidence linking him/her to the crime, distinguishing the suspect from all other

persons as the perpetrator of the crime (Van Graan & Budhram, 2015:47 & 64). Identification which is not followed by individualisation has no evidential value and can at best give direction to an investigation (Marais, 1992:20).

2.4.2 Individualisation

A primary objective of the investigator is to positively identify the individual who has committed the crime (Lee & Harris, 2000:14), hence the importance of identification and individualisation as investigation objectives. Individualisation involves activities aimed at collecting evidence that can prove that a crime has been the act of a particular person or persons, excluding all others beyond the required burden of proof (i.e. the crime is individualised) (Van Graan & Budhram, 2015:46-65). Marais (1992:1, 4 & 19) equates the individualisation of a crime with the positive identification of the offender.

During interviews, eighteen (18) participants provided an accurate description of the concept of individualisation, but the remainder did not know its meaning. All the participants used the term 'positive identification' of a suspect rather than 'individualisation' of the crime. Identification methods which are recognised and accepted by South African courts to positively identify offenders and individualise crimes, include recognition based on a person's physical appearance and characteristics (i.e. direct witness observation, identity parades and photo identification), fingerprints, handwriting, video recordings and deoxyribonucleic acid (DNA) profiling[3] (Schwikkard & Van der Merwe, 2005:367-371).

In Chapter 3 different identification methods related to specific aspects of counterfeit card fraud cases are discussed. Identification methods include:

- A collective analysis of the transaction history of different compromised cards in order to identify the point(s) where the original cards had been compromised and the points where the counterfeit cards were used to commit fraud.

[3] In a SAPS counterfeit card fraud case, Mbuzini CAS 13/01/2012, a bank card which was found in a suspect's vehicle, was positively linked to him on the basis of a positive DNA analysis. The suspect's involvement in the crime could be proven by positively linking him to the card (also see Annexure F as per attached).

- Surveillance of common points of compromise and points of fraudulent spend.
- Fingerprint and DNA examination of counterfeit cards, skimming devices and equipment used by perpetrators to skim and counterfeit cards.
- A digital forensic examination and analysis of counterfeit cards, skimming devices, card encoders, cellphones, computer and related equipment, in order to identify unknown victims and compromised accounts.
- The specific modus operandi, methods and components used to construct skimming devices and PIN-capturing devices.

The discussion which follows focuses on the crime of counterfeit card fraud, its legal elements, modus operandi and the equipment used to commit the crime.

2.5 COUNTERFEIT CARD FRAUD

Counterfeit card fraud is a specific type of fraud involving specific modus operandi and advanced equipment. In order to investigate this crime, it is necessary to understand its legal elements in the context of South African law.

2.5.1 Fraud

Fraud is a crime as old as man. Reference to fraud can be found in various ancient writings. The Quran describes the destruction of Midian (a territory in the Sinai Peninsula neighbouring Canaan) by an earthquake as a result of the Midianites' refusal to cease with their fraudulent practices. Despite the Islam prophet Shoaib's warnings and prophecies (Quran VII, 85-93) the Midian people continued with their dishonest practices, and they were destroyed. In the Torah and the Bible (Genesis 27:1-40) the history of Isaac, Rebecca, Esau and Jacob is told. Jacob (Esau's younger brother), motivated by their mother Rebecca, deceived his father Isaac to obtain the latter's blessing and the birthright that was meant for Esau.

Fraud is defined as the unlawful, intentional making of a misrepresentation, which causes actual prejudice or which is potentially prejudicial to another (Snyman, 2006:523). Burchell (2005:833-835) is in agreement and points out that a specific form of intent is required, namely the intent to defraud. The elements of fraud are unlawfulness, misrepresentation, prejudice and intention. Participants were asked to give their understanding of fraud and its elements. In response to this question, all

the participants were able to give an explanation of fraud and its elements. A discussion of the legal elements of fraud and how they apply to counterfeit card fraud follows.

2.5.1.1 Unlawfulness

The act committed must have been unlawful and no recognised ground of justification must have existed at the time. Although an act or omission may be prohibited by law, its unlawfulness may be excluded if a person can justify the act or omission in terms of recognised principles in law, known as grounds of justification (Burchell, 2005:226). Grounds of justification include self-defence, necessity, acting under orders, consent, supposed defence and public authority (Burchell, 2005:227; Snyman, 2006:36). When counterfeit card fraud is committed, there can be no question that the element of unlawfulness is present. Consent cannot be used as a ground of justification, since it would not have been necessary to counterfeit the original card, had there been consent from the cardholder in the first place. This is also the view of Ferreira (2012:28).

2.5.1.2 Misrepresentation

This element involves the act (conduct) and constitutes the essence of fraud (Burchell, 2005:836). The act can either be a physical action or a failure to act (omission) and must be deceiving or misleading. There must be some sort of untrue, misleading or incorrect statement or presentation of fact or law made to a person or his/her agent. A misrepresentation is a lie, and can be made by words (verbal or in writing), conduct or a combination of the two[4].

Withdrawing money from an ATM or merchant by using a counterfeit bank card, or presenting a counterfeit card to a cashier to pay for goods or services, constitutes a misrepresentation to the bank (by means of the ATM) or merchant in respect of the true identity of the user of the card, purported lawful consent and/or access to the funds in the account linked to the card (Burchell, 2005:840; Snyman, 2006:527)[5]. Therefore, in cases where a counterfeit card is used to commit fraud, the element of misrepresentation is present.

[4] See *R v Larkins* 1934 AD 91 94 and *S v Mbokazi* 1998 1 SACR 438 (N) 445F-I.
[5] This view is confirmed in *S v Myeza* 1985 (4) SA 30 (T), *S v Van den Berg* 1991 (1) SACR 104 (T) and *S v Salcedo* 2003 1 SACR 324 (SCA).

The prosecution will have to prove that the accused was using a counterfeit card and was acting without the cardholder's consent. Evidence that the card is counterfeit and that the physical appearance and features of the counterfeit card differ from that of a genuine card, will have to be tendered. It must be ascertained and proven, through the testimony of the cardholder, that the latter was in possession of his/her own bank-issued card at the time of the fraudulent transaction(s) and did not consent to the fraudulent transaction(s).

An affidavit from the cardholder (account holder), a statement from the bank in terms of section 236 of the Criminal Procedure Act, 1977, and account statements reflecting the fraudulent transactions, as well as the legitimate transactions prior to the fraudulent spend, will be required to prove the element of misrepresentation. A section 236 statement from the bank is also required to authenticate and provide evidence in respect of relevant bank records.

Ferreira (2012:14-15) indicates that, when money or credit is withdrawn or otherwise removed from a bank account without the consent of the account holder by using a counterfeit card, both fraud and theft are committed. However, as Ferreira points out, the mere copying (skimming) or accessing of data encoded on a valid bank-issued card does not constitute fraud or theft, as South African law does not recognise data or information as property that can be stolen, despite its potential value. The prejudice must go further than the unlawful copying of data encoded on a bank card.

2.5.1.3 Prejudice

Prejudice must follow as a result of the conduct of the perpetrator. Merely lying, without any harmful consequences to anyone, is not punishable. Burchell (2005:841) explains that prejudice caused during the commission of fraud can be divided into two broad categories, being proprietary and non-proprietary, and may be actual or potential. Proprietary prejudice is present when the prejudice exists in respect of some sort of property or advantage. Non-proprietary prejudice can exist in relation to non-tangible interests such as reputation, dignity and public administration. If the

public administration is materially inconvenienced or frustrated, leading to potential prejudice, it may constitute fraud[6].

Prejudice must not be too remote or fanciful. Potential prejudice implies that the conduct must have involved a risk of prejudice and that it was reasonably possible that the prejudice would occur (Snyman, 2006:528). If a person's conduct, objectively measured, would reasonably result in prejudice, potential prejudice is present, which is sufficient to satisfy the requirement of prejudice. The prejudice need not be caused to or intended for the party to whom the misrepresentation is made; it could be suffered by a third party or the government.

In counterfeit card fraud cases, the prejudice is actual if the fraudulent withdrawal or purchase is made successfully. If the withdrawal or purchase with the counterfeit card is declined, prejudice is still present but it is potential (this can also be prosecuted as attempted fraud).

2.5.1.4 Intention

The intention required to prove fraud consists of two elements that must both be present – the intent to deceive and the intent to defraud (Burchell, 2005:844; Snyman, 2006:531). Intent to deceive means that the accused must have made some representation knowing or foreseeing that it might be false, and it is his/her intention to make the other party believe something which is not really true[7]. However, intent to defraud goes further. The accused must have the intention to move or convince the party to whom the false representation is made, to act upon it so that the result will be an actual or potential prejudice to himself/herself or another party. To defraud is to deprive by deceit; it is to induce by deceit someone to act to his/her injury.

Intention to deceive is clearly present in counterfeit card fraud, since the fraudster using the counterfeit card makes a misrepresentation to the bank or merchant. By presenting a counterfeit card as genuine and by using the illegally obtained PIN of the actual cardholder to have the transaction authenticated, the fraudster is

[6] This approach was followed by the court in *R v Heyne* 1956 (3) SA 604 (A), where the court held that the failure by the owners of a liquor store to properly keep records of liquor sales, as stipulated by law, amounted to potential prejudice to the state.

[7] In *Re London and Globe Finance Corporation Ltd* 1903 1 Ch 728 the court held that to deceive is to induce someone to believe that something is true which is false.

misrepresenting his/her true identity and is purporting to have legal authority and access to the funds in the victim's account. The intention to defraud is also present, since the fraudster's misrepresentation to the bank or merchant by means of an ATM or point-of-sale (POS) device with regard to the counterfeit card, PIN, his/her identity, consent and legal standing in respect of access to the funds held in the account, is aimed at moving the bank or merchant to authenticate the transaction, which would result in prejudice to the victim, bank or merchant.

2.5.2 Statutory offences related to card skimming

In counterfeit card fraud cases the investigation generally focuses on common law fraud but, depending on the circumstances of a case, the investigator should keep in mind that there are a number of statutory offences related to card skimming which also need to be investigated. Counterfeit card fraud and card skimming investigations should include both fraud and the relevant statutory offences. These include contraventions of certain sections of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) (ECT Act), the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002) (RICA), the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998) and the Customs and Excise Act, 1964 (Act No. 91 of 1964).

Section 86(1) of the ECT Act and section 49(1) of RICA prohibit the skimming (copying) of data encoded on the magnetic strip of a card. In terms of section 86(3) of the ECT Act the possession, producing, selling, offering for sale, procuring, designing, adapting or distributing of a skimming device with the intent to use it for unlawful purposes, is an offence, while section 86(4) prohibits the use of a skimming device. Section 86 and other provisions of the ECT Act are likely to be replaced by similar offences in future (sections 5 to 10 of the Cybercrimes and Cybersecurity Bill, 2015).

In terms of section 49(1) of RICA it is illegal to intercept or use another person to intercept communication without the authority or consent of its author. Section 51(1)(a)(i), read with section 45(1) of RICA, declares it an offence to possess, manufacture, assemble, sell, purchase or advertise any listed electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, which is primarily designed to intercept communications. This includes miniature cameras

and video cameras, keystroke recorders and computer software that can be used to access, record, monitor, retrieve or make available to a person communication-related information without the consent of its author and which can be used as PIN-capturing devices (Government Notice No. R. 1263, dated 29 December 2005, in Government Gazette No. 28371). It is, therefore, clear that it is illegal to possess, buy, sell, manufacture, design, distribute or advertise any card skimming device or PIN-capturing device, if it is meant for unlawful purposes (card skimming, PIN capturing and/or counterfeit card fraud).

Ferreira (2012:55) explains that the import of skimming devices and PIN-capturing devices could be prosecuted in terms of section 81, read with section 15 of the Customs and Excise Act, 1964, for the non-declaration or import of goods prohibited, restricted or controlled by law (i.e. ECT Act and RICA). It must, however, be kept in mind that the intention for possessing the device must relate to an unlawful purpose. In addition, section 83(1)(a) of the Customs and Excise Act, 1964 prohibits a person to possess, have in his/her custody or under his/her control, purchase, sell or dispose of any goods which are illicit goods in terms of the Act (i.e. goods in respect of which any part of the Act is contravened). A person can also be prosecuted for making a false declaration in respect of imported goods (section 84, read with section 15).

Other statutory offences that may have a bearing on counterfeit card fraud cases include contraventions of sections 2, 4, 5 and 6 of the Prevention of Organised Crime Act, 1998, respectively, racketeering, money laundering, assisting another to benefit from the proceeds of unlawful activities, and the acquisition, use and possession of the proceeds of unlawful activities.

2.6 COUNTERFEIT CARD FRAUD MODUS OPERANDI AND EQUIPMENT

It is evident from various sources that one can distinguish three stages or phases in counterfeit card fraud, the first two being preparatory and the third being the actual commission phase, collectively referred to by Divitt (2013:1) as a ‘lifecycle’ (also see Hayes, 2014:8-20; Sabric, 2012:30). The preparatory phases consist of the skimming of an original bank-issued card and capturing/recording the cardholder’s PIN, followed by the manufacturing of a counterfeit card by encoding another card with the skimmed card data. The actual commission of fraud (fraudulent spend) is

the third phase and takes place when the counterfeit card is used to withdraw cash from an ATM or merchant, and/or to make purchases from a merchant. These stages have been corroborated with information obtained from actual cases investigated by the South African Police Service (see Annexure F) and from participants during interviews.

A bank card is issued with security features, which are designed to prevent fraudulent use of the card (Visa USA, 2012:1-2; MasterCard International, 2015:1-2; MasterCard South Africa, 2009:1-2). Security features which are designed to protect authentication data include a magnetic stripe (strip) on the back of the card, an embedded microchip on the front of the card (if it is a smartcard i.e. chip-and-pin card) and a secret PIN, which is linked to the specific card and issued only to the cardholder upon positive verification of identity. Annexure D provides illustrations of the card security features of Visa and MasterCard. During interviews, all the participants have been aware that counterfeit card fraud is made possible when criminals circumvent the security measures provided by the encoded magnetic strip of a card and the secret cardholder PIN.

Smartcards are more secure than magnetic stripe cards in the sense that the embedded microchip (micro-processor) protects and authenticates card and PIN data more securely, thereby helping to prevent counterfeit card fraud (Europol, 2012:5; Smart Card Alliance, 2015:4; Sabric, 2015:4; Heuker, 2013:10-11). However, the magnetic stripe has been retained on smartcards to ensure that they can still be used in countries which are not chip-and-pin (EMV[8]) compliant (Sabric, 2013c:27; Payment Card Industry Security Standards Council [PCI SSC], 2013b:5-7). Figure 1 and Figure 2 of Annexure E, respectively, show examples of magnetic stripe-based cards and chip-and-pin cards. Other visible card security features become relevant only when an exact copy of an entire card is made (whole-card

[8] EMV is a global standard for credit and debit payment cards based on chip card technology, taking its name from the original developers, Europay, MasterCard and Visa. EMV specifications include, but is not limited to, card and terminal evaluation, security evaluation and management of interoperability issues (EMVCo, 2015).

counterfeiting/cloning), which a fraudster can present as payment for purchases at a merchant (see Annexure D as per attached)[9].

2.6.1 Card skimming and PIN capturing

According to Hayes (2014:8) card skimming is performed using three methods, namely handheld skimming (at restaurants, retailers, toll booths and ATMs), overlay devices (ATM skimming, gas pump skimmers and ticket vending machine skimmers) and parasite devices (point-of-sale terminal skimming). Although all three methods are prevalent in South Africa, overlay devices are used mainly for ATM skimming (Sabric, 2015:19-23; Banking Association of South Africa, 2013:1). Between 1 January 2010 and 30 September 2015 a total of 892 handheld skimming devices and 267 ATM-mounted skimming devices were seized nationally. A total of 93 POS skimming devices were seized from 1 January 2013 to 30 September 2015 (Sabric, 2015:23).

During interviews, twenty (20) participants were able to describe all three methods of card skimming. All the participants were able to explain handheld skimming and ATM skimming in detail. Six (6) participants have heard of point-of-sale skimming but did not know how it was committed, while three (3) have never heard of it. As far as the investigation of different types of skimming is concerned, fourteen (14) investigators (five from SAPS and nine bank investigators) indicated that they have investigated all three types of skimming. Ten (10) investigators (five SAPS and two bank investigators) have investigated only handheld skimming and ATM skimming cases, while the remainder have investigated only handheld skimming cases. These figures show that a third of the SAPS investigators have not investigated ATM skimming before and that two-thirds have never investigated POS skimming. Furthermore, a quarter of the bank investigators have also not investigated POS skimming before.

Several participants underlined the importance of an effective investigation in order to identify skimming devices which are recovered, in order to present evidence with regard to the possession and operation thereof. Any skimming device, encoder,

[9] In the case of Kliptown CAS 348/03/2014 a total of 66 Visa and MasterCard hologram stickers were seized from a suspect, together with a handheld skimming device, two portable point-of-sale skimming devices, two card encoders, four laptops, 77 counterfeit cards, and 792 store and gift cards. In Milnerton CAS 733/03/2013 a suspect was arrested collecting a parcel containing a large number of Visa and MasterCard hologram stickers, while 648 counterfeit cards were seized at the suspect's residence.

counterfeit card, keypad overlay, pinhole (micro) camera, computer or any other related equipment used for card skimming, PIN capturing and/or card counterfeiting should, when found, be seized without a search-and-seizure warrant in terms of section 20, read with section 22 of the Criminal Procedure Act, 1977, or section 4 of the Customs and Excise Act, 1964.

A summary of participants' responses indicated that any skimming device, card encoder, counterfeit card, keypad overlay, camera, computer or any related equipment, should upon seizure be examined and analysed by a digital forensic expert to ensure that all stored data is retrieved, and to examine and document the operation of the device or equipment. This is also prescribed by SAPS policy and directives (SAPS, 2010b:1-3; 2011a; 2011b:1-16). Data retrieved from devices and equipment should be followed up by the investigating officer.

In addition, the investigation must include photographing the relevant device/equipment, documenting its physical appearance and fitment to the ATM (where applicable), a fingerprint examination of the device/equipment, the taking of DNA samples from it, a digital forensic examination of the device/equipment, and an analysis of available surveillance camera footage. An examination of the ATM by an installation/maintenance technician and a bank investigator might also be required.

Investigators need to be knowledgeable with regard to the different types of skimming prevalent in South Africa. A counterfeit card fraud case cannot be investigated successfully if the investigator does not know how the fraud was committed, what equipment and technology were used, and what evidence to look for. The three methods of card skimming prevalent in South Africa will now be discussed.

2.6.1.1 Handheld skimming and PIN capturing

When handheld skimming takes place, a small card reader is held in the hand and the original card data is skimmed (copied) by unobtrusively swiping the magnetic stripe through the card reader slot (Hayes, 2014:7-10; Sabric, 2015:21-22). The skimming device is battery powered and has memory storage capacity. Handheld skimming devices vary in size; some are smaller than a bank card and can easily be hidden in a pocket (also see Annexure E as per attached).

Handheld skimming can be performed in venues where an original card is tendered as payment and a cashier or waiter discreetly swipes the card through the skimming device. Cardholders could be targeted at restaurants, toll booths, retail stores, shops and filling stations. The cardholder's PIN is observed when entered onto the point-of-sale terminal. Handheld skimming also takes place at ATMs when a client is distracted or offered unsolicited help (Sabric, 2013a:1). The victim's card is skimmed with a handheld device and his/her PIN is obtained through observation when it is entered onto the keypad of the ATM ('shoulder surfing') (see Annexure F for examples of such cases). Handheld skimming even takes place inside banks where bank officials have been found to skim clients' cards[10].

2.6.1.2 ATM-mounted skimming and PIN capturing

ATM skimming involves a card reader and a PIN-capturing device which are attached to an ATM (Sabric, 2014:23; 2015:22-23; Krebs, 2010a:1-2; 2011b:1-3). The skimming device (card reader) is fixed onto or over the original card slot (bezel) of the ATM to enable the device to read the magnetic strip of a card that is inserted into the slot. The PIN-capturing device is either a miniature (pinhole) camera or a keypad overlay. A miniature (micro) camera is placed in a position to enable it to record keystrokes (the PIN) entered onto the keypad. The camera is often placed at the back of a tiny hole behind a fixed panel or inside a brochure rack.

Alternatively, the PIN is recorded by means of a keypad overlay, which is essentially a false numeric keypad placed on top of the real keypad and fixed to the ATM (Hayes, 2014:9-13)[11]. Skimmed card data and captured PINs are retrieved when the skimming device and PIN-capturing device are removed from the ATM. Technologically advanced ATM skimming devices can transmit skimmed card and PIN data by means of bluetooth, wireless fidelity (wi-fi) or 'global system for mobile communications' (GSM) networks to a fraudster's cellphone, making it available in real-time (Krebs, 2010b:2; 2015:1-3; Feinberg, 2014:1-7). Figures 4 to 6 in Annexure E portray ATM skimming devices and PIN-capturing devices.

[10] Delmas CAS 43/01/2012, Wierdabrug CAS 205/03/2013, Hendrina CAS 68/04/2012

[11] In Humewood CAS 64/11/2014 a battery powered false keypad overlay was seized, which had the capability to store data digitally.

Fraudsters often manufacture their own ATM skimming devices and PIN-capturing devices. Several 'home factories' have been found which were used for the manufacturing of skimming devices, PIN-capturing devices and counterfeit cards[12].

2.6.1.3 Point-of-sale skimming and PIN capturing

Point-of-sale skimming involves any of four methods, as described by Krebs (2011a:1; 2013a:2; 2013b:2) and the Payment Card Industry Security Standards Council (2009:15), namely:

- A standard point-of-sale device that has been tampered with and converted into a skimming device.
- A point-of-sale device of which the software has been infected and altered to transmit skimmed card and PIN data to the fraudster over a computer network, using bluetooth or wi-fi transmission.
- A card and PIN data logger which is attached to a cash register.
- Intercepting legitimate real-time wireless (mobile) data communications from POS devices at merchants via bluetooth or wi-fi transmission.

In Figures 7 and 8 in Annexure E, examples are shown of point-of-sale skimming technology. According to Krebs (2012:1) a standard POS device can be adapted for skimming in such a manner that, once the card has been swiped and the PIN entered, the device prints a 'connection error' or 'offline' receipt (also see Sabric, 2015:23). The customer is then informed that the POS device is offline or out of order and the card is swiped again, this time using a legitimate POS terminal. The card and PIN data is stored by the adapted POS device which was first used. This modus operandi has been confirmed in various cases[13].

MasterCard International (2009:11-12) explains that criminals obtain original point-of-sale devices by stealing or purchasing one. The device is then disassembled and reverse engineered, adapted and returned to the merchant location or introduced at another location by replacing a legitimate POS device with the adapted one.

[12] Including Umhlali CAS 6/10/2014, Norwood CAS 383/07/2012, Bedfordview CAS 162/10/2013, Sandton CAS 411/04/2013 and Randburg CAS 466/04/2013.
[13] Including Garsfontein CAS 572/08/2013, Parkview CAS 84/10/2013, Wierdabrug CAS 644/10/2013 and Witbank CAS 1045/10/2013.

Mobile POS devices communicate using cellphone networks and protocols (PCI SSC, 2009:15). However, they are normally also bluetooth and wi-fi enabled, and these data communications can be intercepted by criminals well beyond the walls of a building. A criminal in the vicinity of an altered mobile POS device can use a bluetooth or wi-fi enabled device, such as a cellphone, to receive skimmed card and PIN data which has been transmitted.

2.6.2 Counterfeiting the card

Once the card data has been copied from a genuine card and the cardholder's PIN obtained, a counterfeit card is produced by encoding the magnetic stripe of another card with the skimmed card data. Counterfeit cards are produced by encoding lost, stolen or other magnetic stripe cards, including white plastic cards, gift cards and store cards (Sabric, 2012:30; 2014:19). The card writer is connected to a computer and uses applicable software to transfer the skimmed card data (which is retrieved from the skimming device) to the counterfeit card. Figures 1, 9 and 10 in Annexure E show examples of magnetic stripe cards, card reader/writer combinations used to read and encode magnetic stripe cards, and counterfeit cards with PIN numbers. Card readers (skimming devices) and card writers (encoders) have been seized in various cases[14].

2.6.3 Fraudulent spend

Up to 85% of fraudulent spend with counterfeit cards are cash withdrawals from ATMs (Sabric, 2013c:1-20; 2014:11-18). However, counterfeit cards can also be used to make fraudulent purchases. During interviews, bank investigators referred to fraudulent spend as 'negative spend' and explained 'positive spend' as legitimate transactions made by the cardholder prior to the fraudulent spend. All of the participants referred to the fraudster who makes the fraudulent withdrawals or purchases as a 'runner'.

During discussions relating to fraudulent spend, ten (10) participants raised an issue, which related to the time of the day when fraudulent withdrawals are made. They indicated that fraudulent withdrawals often take place just before and after midnight, since the runner wants to withdraw the maximum daily amounts allowed on the

[14] Including Pretoria West CAS 591/05/2013, Dunnottar CAS 44/07/2013, Daveyton CAS 240/09/2013 and Humewood CAS 454/06/2011 (also see Annexure F as per attached).

victim's account in the shortest time possible. In this way, a runner can withdraw the maximum amount allowed for two consecutive days within a few minutes. During the docket analysis, this was found to be true in 12 of the 100 dockets analysed[15]. In other cases fraudsters used counterfeit cards to pay for goods and services at merchant venues[16].

One of the bank investigators interviewed commented that the point of compromise of the original card is often different from the point where the fraudulent spend takes place (i.e. two different crime scenes). Evidence for this was found during the docket analysis. In 35 out of the 100 dockets analysed it was clear that the original cards had been compromised in different geographical locations than where the fraudulent spend took place[17].

On the issue of fraudulent spend, fourteen (14) participants also pointed out that, while cards and PINs are compromised in South Africa, the fraudulent spend often takes place in other countries, which means that it is likely that the skimmed card data and PIN are forwarded to someone in another country, who counterfeits the card and commits fraud. During docket analysis, four (4) such cases were identified[18]. In one case[19] a total of 17 fraudulent POS purchases were made over four days, using counterfeit cards in Spain, the United States and Hong Kong (also see Sabric, 2013b:1; 2014:8 & 12). In other cases[20] arrests were made when suspects presented counterfeit international cards as payment.

Evidence relating to fraudulent withdrawals and purchases with counterfeit cards can be obtained in terms of section 205 of the Criminal Procedure Act, 1977 and include the following (SAPS, 2010d; 2011b; 2013c):

[15] Including Hillbrow CAS 913/01/2013, Johannesburg Central CAS 1307/02/3013 and Norwood CAS 202/03/2013).
[16] Including Roodepoort CAS 856/10/2013, Bedfordview CAS 334/09/2013 and Sunnyside CAS 490/11/2013.
[17] Including Booysens CAS 353/02/2013, Brixton CAS 497/01/2013, Johannesburg Central CAS 1359/01/2013 and Sandton CAS 762/01/2013.
[18] Johannesburg Central CAS 520/12/2012, Rosebank CAS 31/02/2013, Sandton CAS 183/01/2013 and Sandton CAS 560/01/2013.
[19] Sandton CAS 183/01/2013.
[20] Edenvale CAS 271/09/2013, Pretoria Central CAS 847/11/2013 and Pretoria Central CAS 886/11/2013.

- Bank statements of the positive (prior to fraud) spend and negative (fraudulent) spend, accompanied by a section 236 (Criminal Procedure Act, 1977) statement from the bank. The account holder must identify the fraudulent spend transactions.
- Information from the bank relating to the unique identity of the ATM (where applicable) and the electronic journal of the ATM showing exact dates and times of fraudulent transactions. The electronic journal of an ATM is a computerised record (log files) of all transactions taking place at the ATM, including lawful spend and fraudulent spend (TestLink, 2014:1; CashCard, 2012:4). Transaction-related information is saved to the ATM's hard drive and can be downloaded or printed by the bank.
- Information from the bank relating to the identity, name and contact details of the merchant (if fraudulent purchases were made).
- Information from the bank with regard to other bank accounts that have been compromised and in respect of which complaints of fraudulent transactions have been reported to the bank in the same area and over the same period. This information must be obtained with a view of determining a possible common point of compromise of the cards and common points of fraudulent spend.
- In the case of fraudulent purchases, identifying information from the merchant relating to the specific point-of-sale terminal and particulars of the cashier involved, with proof that the cashier was on duty at the time at that terminal. The transaction slips and sales dockets relating to the fraudulent purchases can give an indication of the cashier's possible involvement and whether prescribed procedures were followed.
- Surveillance footage. Surveillance cameras can provide recorded footage of activities taking place inside a merchant location on the specific date and time when the fraudulent purchase was made, including surveillance of the specific pay point. Surveillance footage recorded at an ATM where a fraudulent withdrawal was made or in shopping malls and around parking areas, should be obtained with a view of identifying suspects and vehicles used by suspects.

2.7 SUMMARY

In this chapter, the concepts of ‘forensic investigation’ and ‘forensic science’ were explained. The differences and interaction between them were discussed. The responsibility, powers and mandate to investigate crime and more specifically, counterfeit card fraud, as it relate to the South African Police Service and bank investigators were considered. The purpose and objectives of forensic investigation with reference to counterfeit card fraud, and the importance of the investigation objectives relating to identification and individualisation were discussed.

This was followed by a discussion of fraud and its legal elements, counterfeit card fraud and related statutory offences. The three phases of counterfeit card fraud were explored, namely: the skimming (copying) of the card data of a valid, bank-issued card and capturing of the cardholder’s PIN, the manufacturing of a counterfeit card by encoding another card with the skimmed card data, and the fraudulent spend phase where the counterfeit card is used to make withdrawals or purchases.

The next chapter will take a closer look at the investigation objectives of identification and individualisation in counterfeit card fraud cases. Different identification methods relating to specific aspects will be examined and evaluated, including the victim, the perpetrators and the points of compromise and fraudulent spend.

CHAPTER THREE:
IDENTIFICATION IN COUNTERFEIT CARD FRAUD CASES

3.1 INTRODUCTION

Any crime can be seen as an event with four separate yet interconnected dimensions, being the law that defines the act to be criminal, the offender, the victim or target, and the simultaneous convergence of these three at a specific geographical (spatial) node (Breuer, Hursey, Stroman & Verma, 2008:2).

The abilities to solve a crime and to develop preventive methods depend on whether the investigator is able to answer the six 'W' questions with regard to the criminal incident: What happened (how did it take place)? Who was the victim? Where did it take place? When did it take place? Who did it? Why did it happen? These questions require the investigator to identify the crime, the victim, the crime scene, the date and time of the incident, the offender, and his/her modus operandi, equipment, actions, involvement and motive. Identification-related activities are, therefore, the key drivers which direct the investigator's quest to find answers.

In this chapter, the use of different identification methods to investigate counterfeit card fraud will be examined more closely. There are various aspects related to any counterfeit card fraud incident, which may have to be identified in order to individualise the crime (see paragraph 2.4.1). Different identification methods may be necessary to identify certain aspects of the crime, depending on the particular case setting and background with which the investigator is dealing. The ultimate goal of the investigator is to collect sufficient evidence, which identifies relevant aspects of the crime positively, to enable the state prosecutor to prove the role which each accused played in the commission of the fraud.

3.2 IDENTIFICATION IN COUNTERFEIT CARD FRAUD CASES

Identification-related activities aimed at achieving the objectives of identification and individualisation are among the most critical to be completed successfully by the investigator and form the basis of any investigation (Marais, 1992:5 & 20; Van Graan & Budhram, 2015:46-47). Identification can generally be typed as direct or indirect identification and divided into eight categories, which are associated with specific

methods of identification. Investigators need to be knowledgeable as to what these categories and methods entail, and which will be appropriate and effective for the specific case under investigation.

3.2.1 Categories and aspects for identification in counterfeit card fraud cases

Identification can be divided into the following categories (Van Graan & Budhram, 2015:48-63; Marais, 1992:2-4; Van der Westhuizen, 1996:6-7):

- Situation identification.
- Victim identification.
- Witness identification.
- Perpetrator (culprit) identification.
- Imprint identification.
- Origin identification.
- Action identification.
- Cumulative identification.

During interviews, twenty-four (24) participants listed victim identification, suspect (perpetrator) identification, witness identification and imprint identification as categories of identification. Four (4) of the 24 participants also included origin identification. Three (3) participants only mentioned suspect identification. None of the participants mentioned situation identification, action identification or cumulative identification. It was evident from responses that participants were mainly conversant with identification categories relating to the victim, perpetrator, witnesses and imprints. In counterfeit card fraud cases, depending on the specific case situation, there are generally three main categories that need to be identified, namely the crime scenes, the role players (victims, criminals and witnesses) and the equipment used (Hayes, 2014:8-20; Sabric, 2012:30) (also see Annexure F as per attached).

A number of aspects specific to counterfeit card fraud, which need to be identified positively during investigation, were established from responses received from participants (see in brackets below), various SAPS reports (see Annexure F) and case dockets analysed (also see SAPS, 2013c:1-6; Pillay, 2011:3; Hayes, 2014:1-

20). Depending on the circumstances of a case, the following aspects would have to be identified positively during investigation:

- The modus operandi, type of skimming, skimming device and PIN-capturing device used (26 participants).
- The person who used the skimming device and PIN-capturing device to illegally obtain the card and PIN data (25 participants).
- The person(s) who performed the fraudulent transactions (25 participants).
- The point(s) of fraudulent spend (merchant(s) and/or ATM(s)) (24 participants).
- The point of compromise of the original card or a common point of compromise of various compromised cards (i.e. common point of purchase) (23 participants).
- The person who manufactured the counterfeit card(s) (22 participants).
- The place where the counterfeit card(s) was/were produced (19 participants).
- The equipment used to manufacture the counterfeit card(s), including the card encoder, computer equipment and, where applicable, card embosser and tipper (18 participants).
- The counterfeit card(s) which was/were used (18 participants).
- The fraudulent (disputed) transactions (fraudulent/negative spend) (18 participants).
- The specific point-of-sale terminal and cashier at a merchant venue where the counterfeit card was presented (16 participants).
- The person who supplied or manufactured the skimming device and PIN-capturing device (16 participants).
- The cellphone numbers of perpetrators and their communications with each other (16 participants).
- The equipment and materials used to manufacture the skimming device and PIN-capturing device (14 participants).
- The place where the skimming device and PIN-capturing device were manufactured (14 participants).
- The prior to fraud transaction history (positive spend) (12 participants).

- The crime (identifying the crime as counterfeit card fraud) (10 participants).
- Any other person who colluded to commit the crime, including those who shared in the proceeds (6 participants).

As far as counterfeit card fraud cases is concerned, it was established that the DPCI follows a national strategy and standard operating procedure (SOP) in respect of the investigation of these cases, which focus more on skimming modus operandi and cooperation with other role players than on appropriate identification methods (SAPS, 2009d:1-12; 2011b:1-16). However, DPCI procedures do prescribe the use of surveillance and digital forensic analysis as possible identification methods (see paragraphs 3.2.1.2 (a) and 3.2.1.3 (c) in this regard). The following discussion will focus on different identification categories and methods in counterfeit card fraud cases relating to the aspects listed above.

3.2.1.1 Situation identification in counterfeit card fraud cases

Van Graan and Budhram (2015:49) describe situation identification as an evaluation of the circumstances and evidence found by the investigator in a specific situation and, based upon own observations, investigative knowledge and experience, firstly deciding whether an incident has taken place or a crime was committed and, if so, what type of incident or crime (also see Adams, Caddell & Krutsinger, 2004:10; Lee, Palmbach & Miller, 2003:27). Hence, knowledge of the crime and its elements, supported by practical experience of crime scenes and situations, are necessary for an accurate situation identification.

From summarised responses of participants and an analysis of official SAPS reports and case dockets (see Annexure F and the list of dockets analysed as per attached), it was established that counterfeit card fraud cases manifest as any of the following situations or a combination of two or more:

- A complaint from a cardholder who has suffered a loss on his/her bank account has been received by the bank or SAPS (in these cases, the suspect, method of skimming and point of compromise of the card are usually unknown).
- Information relating to card skimming and/or counterfeit card fraud activities has been received or collected by the bank or SAPS.

- A counterfeit card, skimming device, and/or PIN-capturing device has/have been seized.
- A suspect has been arrested on suspicion of card skimming and/or counterfeit card fraud.

The initial circumstances of a case and the changing situation as the investigation progresses and develops will dictate the necessity and scope of identification-related activities. During interviews, 26 of the 29 participants (which included both Sabric participants) indicated that complaints from cardholders who have suffered losses on their accounts, where the perpetrator(s), method of skimming and point of compromise of their card are unknown, are the most common manifestation of counterfeit card fraud. The different stages of counterfeit card fraud, as discussed in paragraph 2.6.1, are likely to take place on different dates and at different geographical locations. Investigators should be able to identify the scene positively where the card and PIN were compromised, the scene where the counterfeit card was produced and the scene where the fraudulent spend took place.

(a) Interviewing the victim

The purpose of an interview with the victim/complainant in a counterfeit card fraud case is to collect evidence and relevant information with regard to the crime (Giacalone, 2015:1-2; American Institute of CPAs, [sa]: 2). The victim can make a valuable contribution to help identify the crime and situation with which the investigator is dealing and to provide a background of the sequence of events: the what, when, where, why, who and how of the crime. In support of this, both Sabric participants pointed out that a thorough interview with the complainant is the most effective method to assess the complaint and to achieve an accurate situation identification. During the interview, it should be confirmed that the complainant was in possession of a valid bank-issued card at the time of the fraudulent transaction(s), that no one had permission to perform the disputed transaction(s) and that no other person had lawful access to his/her PIN.

It should be established whether the complainant had encountered any suspicious or out of the ordinary behaviour from someone when using an ATM or point-of-sale device prior to the fraud, or was offered unsolicited help at an ATM. Furthermore, it should be established whether, prior to the fraudulent transaction(s), an ATM had

retained his/her card, whether the complainant's card was removed from his/her sight or whether a cashier or waiter had exchanged POS devices during a transaction. These might all be indicative of card skimming and may help to identify the point of compromise of the card.

During the interview, the complainant should be requested to identify the fraudulent transaction(s) on his/her bank statements and provide a transaction history of positive spend for analysis purposes, in order to identify a possible point of compromise (SAPS, 2011b:1-6; Pillay, 2011:3). During the docket analysis, it was found that in only nine (9) of the 100 counterfeit card fraud dockets the cardholder was interviewed by the investigating officer.

3.2.1.2 Victim identification in counterfeit card fraud cases

Victim identification includes activities and action steps to establish who the primary victim or target of a crime was (Marais, 1992:4 & 24-39). In counterfeit card fraud cases victim identification usually does not pose a problem to investigators. There was general consensus among participants that in practice victims contact their bank as a first point of entry to report fraudulent (disputed) transactions on their accounts, since the victim wants his/her card to be blocked and wants to be reimbursed for the loss. However, a counterfeit card or skimming device may be recovered and the cardholder(s) of the compromised card(s) might be unknown, in which case the investigator will have to identify the victim(s) (see Annexure F as per attached).

During interviews, investigators were asked how they would identify unknown victims of counterfeit card fraud. The following responses were received:

- A digital forensic analysis of counterfeit cards, skimming devices and/or related equipment which are recovered (20 participants).
- With information and the assistance of the bank (18 participants).
- An analysis of merchant transaction vouchers and/or the ATM electronic transaction journal (8 participants).

(a) Digital forensic analysis

A digital forensic analysis relates to the expert examination and analysis of digital (electronic) media with the object of identifying, recovering, preserving and

documenting digital evidence, which is stored as electronic or magnetically encoded data, and to present facts and expert opinions in court in this regard (United States Computer Emergency Readiness Team, 2008:1; Jordaan, 2015:364-392). Digital evidence includes any document, text, message, communication or presentation which is in electronic format, and which may exist on any electronic device or storage medium capable of storing or processing digital information, including bank cards, skimming devices, PIN-capturing devices, card writers, computers, cellphones, external hard drives, memory sticks (flash disks/drives), compact discs and memory cards.

Both SAPS and bank investigators have access to private digital forensic analysis service providers (SAPS, 2010b:1-3; 2010c:1; 2011b:1-16; 2013c:1-4). Furthermore, SAPS investigators can make use of digital forensic analysts and services provided by the SAPS Cyber Crime Intelligence Support Section and trained digital crime scene first responders. Digital forensic analysis tools (e.g. XRY and Analyst Workstation) are available in the SAPS to extract and analyse cellphone data (Schmitz & Cooper, 2015:327-328).

In terms of national SAPS directives a digital forensic analysis of all recovered skimming devices, PIN-capturing devices and related card counterfeiting equipment is compulsory, in order to identify victims and provide evidence of the operation and contents thereof (SAPS, 2010b:1-3; 2013c:1-4). Data retrieved from a skimming device, counterfeit card, card encoder or a suspect's computer, could be used to identify victims effectively by means of skimmed card data, which should include the primary account number (PAN) of the cardholder (see Annexure F as per attached). Furthermore, skimmed card data retrieved from a counterfeit card can confirm that the card is counterfeit. Noteworthy cases where skimmed card data was retrieved by means of a digital forensic analysis and used to identify victims and counterfeit cards successfully, include Mount Road CAS 387/04/2011[21] and Sandton CAS 441/04/2013[22].

Twelve (12) participants (which included both Sabric participants) emphasised the importance of following the correct procedures when seizing skimming and PIN-

[21] Skimmed data of 1 490 cards was retrieved from an ATM skimming device.
[22] Skimmed data of 2 364 cards was retrieved from four ATM skimming devices.

capturing devices, counterfeit cards, card encoders, computers and related equipment. Exhibits must be photographed where they are found, documented, examined for fingerprints, and packaged and sealed correctly in exhibit bags for submission to the digital forensic analyst (also see Jordaan, 2015:386-388).

(b) Analysis of merchant transaction vouchers and the ATM electronic transaction journal

Eight (8) participants suggested an analysis of merchant transaction vouchers or the electronic journal of the ATM as a method to identify victims, depending on where the card(s) was/were compromised. In the case of Kareedouw CAS 49/08/2011 it was shown that compromised accounts and, therefore, victims could be identified successfully by using information which was retrieved from an ATM electronic transaction journal by the bank[23].

Once a common point of compromise at a merchant venue or ATM has been identified, details of all transactions performed and cash dispensed (including card numbers and account numbers linked to compromised cards) can be obtained from the merchant point-of-sale transaction vouchers or the electronic journal of the relevant ATM for the specific date(s) on which card skimming is suspected to have taken place. This information can be used to verify and follow up disputed (fraudulent) transactions (CashCard, 2012:4). With the assistance of the bank, card numbers and linked account numbers can be used to identify victims of card skimming at a common point of compromise.

3.2.1.3 Perpetrator (culprit) identification in counterfeit card fraud cases

Establishing the identity of the perpetrator is a decisive factor in solving a crime. Perpetrator identification involves collecting and evaluating information and facts aimed at positively determining the identity of the perpetrator, and includes direct and indirect methods (Marais, 1992:5 & 22; Lee et al, 2003:24; Van Graan & Budhram, 2015:55-63). Direct identification methods include direct recognition by the victim and/or eyewitnesses on the basis of physical appearance, race, gender and/or age, identification parades, photographic identification (including video camera surveillance footage and photo identification parades), voice identification, modus

[23] To this end, also see Uitenhage CAS 426/01/2012, Sea Point CAS 284/05/2013 and Kwazekele CAS 569/08/2010.

operandi and trademarks of the perpetrator. Indirect ways of perpetrator identification involves physical evidence which can be positively linked to the perpetrator (including handwriting, fingerprints, shoe prints, tyre tracks, tool marks, fibres, serial numbers and DNA from bodily fluids and tissue) (Van Graan & Budhram, 2015:63).

It was established from participant interviews and various SAPS reports (see Annexure F as per attached) and directives (SAPS, 2009d; 2010b; 2013c:1-6), that a number of methods exist which can be used to identify perpetrators positively in counterfeit card fraud cases. These methods are supported by Sabric (2013d:1), Pillay (2011:3) and Verafin (2011:3-7) (also see Manamela, Smith & Mokwena, 2015:110-115). Perpetrator identification methods include the following:

- Identifying common points of fraudulent spend, supported by surveillance to identify previously known fraudsters and suspects acting suspiciously (e.g. making multiple withdrawals using different cards, withdrawing money around midnight or obscuring their faces from surveillance cameras) (16 participants).
- Identifying a common point of compromise of different cards, which have been compromised in the same geographical area over the same period, supported by surveillance to identify previously known suspects and suspects behaving suspiciously (including card skimming, shoulder surfing, loitering in the vicinity of an ATM or persistently offering unsolicited help to others) (16 participants).
- The purposeful surveillance of popular and frequently used ATMs and merchant venues in order to identify previously known suspects, as well as suspicious actions related to card skimming and PIN capturing (15 participants).
- A thorough interview of all suspects arrested and obtaining information in order to identify other suspects (15 participants).
- Call data and cellphone handset usage analysis of suspects in order to identify accomplices by means of contact details and communications (13 participants).
- Fingerprint examination and analysis in respect of recovered counterfeit cards, skimming and PIN-capturing devices, false panels and overlays,

components and related equipment in order to identify suspects from existing criminal databases (10 participants).

- DNA profiling (3 participants).
- Profiling of suspects (2 participants).

(a) Identifying the point of fraudulent spend

The point of fraudulent spend refers to any merchant venue or ATM where a fraudster uses a counterfeit card to purchase goods or withdraw cash (Esker, 2013:1-3; Hayes, 2014:7-15). During interviews, participants were asked how one could identify the point(s) of fraudulent spend or a common point of fraudulent spend during the investigation of counterfeit card fraud cases. The following identification methods were provided by participants:

- An interview with the victim (cardholder) during which negative spend (fraudulent transactions) should be identified from relevant bank statements. Information identifying the specific point(s) of fraudulent spend (merchant or ATM) should be obtained from the bank statements. Should the bank statements be inadequate to identify the point(s), additional information must be obtained from the bank (19 participants).
- Surveillance of suspected points of fraudulent spend in order to identify suspects behaving suspiciously (e.g. making multiple withdrawals using different cards at the same ATM, making withdrawals at midnight or obscuring their faces from surveillance cameras) (16 participants).
- A collective analysis of negative (fraudulent) spend transaction data relating to different cards which have been compromised in the same geographical area over the same period (12 participants). Sources, tools and aids which can be used to perform such an analysis, include bank statements, Microsoft Excel spreadsheets, i2 Analyst's Notebook and Sabric analysts.
- The thorough interviewing of suspects in custody in order to identify points of fraudulent spend (10 participants).
- Identifying common points of fraudulent spend (fraud hotspots) from the Tactical Weekly Provincial Commercial Crime Risk Forecast, which is

compiled by Sabric and distributed to SAPS and bank investigators (see Annexure G as per attached) (7 participants).

During interviews, sixteen (16) participants indicated that a positive perpetrator identification could be achieved by identifying points of fraudulent spend and placing them under surveillance. Surveillance activities should focus on identifying previously known fraudsters and suspects who act suspiciously. It has been proven that surveillance of a positively identified common point of fraudulent spend can be used as a method to identify perpetrators positively[24] (also see Annexure F as per attached). It is, therefore, important that investigators should know how to identify points of fraudulent spend and common points of fraudulent spend.

Heuker (2013:11) supports a collective analysis of fraudulent spend transaction data relating to different compromised cards to identify common points of fraudulent spend during investigation (also see Detica, 2010:1). In order to do this, fraudulent transactions should be identified by account holders from their bank statements, captured on a collective database or retrieved from the bank's existing database and analysed to identify common points of fraudulent spend. MasterCard International (2010a:1; 2010b:4) and 3VR Incorporated (2011:2) advocate the use of real-time transaction surveillance and analysis systems, supported by and integrated with camera surveillance, to identify points of fraudulent spend and perpetrators.

Hill and Paynich (2014:9 & 220) contend that operational (tactical) crime information analysis and crime mapping can be used to solve cases by identifying clusters of criminal activity, crime threats, crime patterns and hotspots, suspects, investigative leads, and spatial relationships between crime incidents and geographic variables. This is done by examining recent criminal events in terms of relevant variables, including the method used (modus operandi), point of entry, instruments used, offender profile and description, day of the week, date, time and location of the crime incident.

In this regard, Sabric produces a weekly report indicating the most common points of fraudulent spend in each province which, as pointed out by participants, is provided to SAPS and bank card fraud investigators on a weekly basis (SAPS, 2011b:1-16).

[24] Uitenhage CAS 426/01/2012, Queenstown CAS 29/11/2011 and Algoa Park CAS 154/08/2010.

Annexure G is an example of a Sabric Tactical Weekly Provincial Commercial Crime Risk Forecast in respect of Gauteng province for the period 23 June 2013 to 29 June 2013.

Investigators can use the Sabric weekly report to guide their investigations in identifying points of fraudulent spend and possible suspects. The Sabric Tactical Weekly Provincial Commercial Crime Risk Forecast provides investigators with detailed information relating to merchant venues and ATMs most targeted by card fraudsters for fraudulent purchases and cash withdrawals, in terms of geographical location, patterns and tendencies. From Annexure G the most prevalent day of the week, time of the day and most targeted ATMs can be seen.

The SAPS also prescribes the use of a crime information analysis process, consisting of a crime threat analysis, crime pattern analysis and crime mapping using the Geographic Information System to identify crime hotspots (flashpoints) and link similar cases (SAPS, 2013d; 2011e; 2011f:4-7). Every police station must have a crime information official (CIO) who is responsible for the daily management, collection, analysis and interpretation of crime information in that area, and to brief investigating officers and patrol officers with regard to the findings of the crime information analysis. This includes a crime pattern analysis and mapping of counterfeit card fraud incidents. Based on this knowledge, resources should be applied more effectively during the investigation and prevention of crime. However, during interviews, only two of the SAPS participants were aware of the existence and role of station CIOs in identifying points of fraudulent spend in counterfeit card fraud cases.

Various analytical tools are available in the SAPS to analyse negative spend and positive spend transaction data from victims' bank statements, and to analyse crime information from the Crime Administration System, relevant databases and systems (e.g. the Inkwazi system). These tools include computer spreadsheet applications (e.g. Microsoft Excel), IBM i2 Analyst's Notebook, i2 iXa and iXv Visualiser (SAPS, 2006a:1-3; 2007:1-2; Schmitz & Cooper, 2015:336-338; Smith & Zinn, 2015:431-432). Annexure H is an example of crime pattern analyses and crime maps, generated with the GIS of the SAPS, using CAS data which was exported to a spreadsheet and sorted alphabetically according to crime scene addresses. It relates

to fraud cases which were reported at the Daveyton police station between 1 June 2013 and 30 June 2013, and between 23 June 2013 and 29 June 2013 respectively.

A comparison of Annexure G and Annexure H as per attached shows that the fraudulent withdrawals reported by Sabric for the period 23 June 2013 to 29 June 2013, relating only to the two ATM hotspots in Daveyton, were 66 compared with the seven (7) fraud cases reported to the SAPS for the entire Daveyton policing area. A possible explanation for the difference is that victims tend to report counterfeit card fraud to their banks, which in turn report it to Sabric. However, victims do not always report the matter to the SAPS. It is also possible that more than one fraudulent withdrawal (fraud incident) could have been made from the same complainant's account. Annexures G and H illustrate that both SAPS and Sabric crime pattern analyses and crime maps can be used to identify common points of fraudulent spend.

In contrast to this, the docket analysis showed that a positive identification of the point of fraudulent spend, on a single case-by-case basis, was achieved in only 28 of the 100 cases analysed. In 14 of the 28 cases, the point of fraudulent spend was identified by SAPS investigators based on information obtained from the cardholder's bank statements. In the other fourteen (14) cases, the point of fraudulent spend was identified by the bank and relayed to the cardholder. There was no indication in the remaining 72 case dockets that a Sabric Tactical Weekly Provincial Commercial Crime Risk Forecast, a crime pattern analysis or crime map was used to identify points of fraudulent spend. None of the 100 dockets analysed were included in any collective analysis of negative spend transaction data in order to identify common points of fraudulent spend.

(b) Identifying a common point of compromise

The point of compromise is the merchant location or ATM where a victim's card is compromised, i.e. the point where the skimming and PIN capturing take place. In practice different cards can be compromised at the same point, which is referred to as a common point of compromise or common point of purchase (CPP) (Rowsell, 2013:1-2; Divitt, 2013:1; Verafin, 2011:3-7). When asked how one could identify the point of compromise or a common point of compromise during counterfeit card fraud investigations, participants volunteered the following methods:

- An interview with the victim during which positive spend (legitimate transactions prior to fraudulent transactions) should be identified from relevant bank statements (18 participants). The process is similar to that of identifying the point of fraudulent spend; however, here positive spend data is used. During the interview, attempts should be made to identify possible points of compromise (see paragraph 3.2.1.1 (a)).
- Surveillance of suspected points of compromise in order to identify suspects behaving suspiciously (e.g. performing card skimming and/or PIN-capturing activities, persistently offering unsolicited help to cardholders, obscuring their faces from surveillance cameras and/or loitering in the vicinity of an ATM) (16 participants).
- A collective analysis of positive spend transaction data relating to different cards which have been compromised in the same geographical area over the same period, based on victims' bank statements. The same tools and aids which are used to identify common points of fraudulent spend, apply here (11 participants).
- A thorough interview of suspects in custody in order to identify points of compromise (10 participants).

Pillay (2011:3) and Verafin (2011:3-7) describe how a CPP can be identified by means of a collective analysis of positive spend transaction data of different compromised accounts (CPP analysis). They advocate the identification of CPPs in counterfeit card fraud investigations to enable investigators to focus their time and resources on identifying perpetrators who are active at CPPs (also see Visa International, 2012). Once a CPP has been identified, it should be placed under surveillance. The identification of CPPs enhances and improves efforts to identify perpetrators, helps to optimise police and bank resources, and prevents further card skimming and PIN-capturing activities.

A CPP analysis is typically done using a tool such as a spreadsheet, a transaction monitoring and analysis system, Analyst's Notebook or similar application. It requires transaction data, which includes the primary account number, ATM identifiers (e.g. number, name and location), merchant identifiers, point-of-sale device identifiers, transaction type/code, reference number, date and time (Ablett, 2014:2; Forman,

2005:1; Zoldi, Wang, Sun & Wu, 2007:1). In addition, the PCI SSC (2013a:9 & 15) and Diebold Incorporated (2014a:1; 2014b) suggest frequent and thorough manual inspections of ATMs by bank or security personnel as a means of identifying points of compromise, by physically detecting skimming devices and PIN-capturing devices attached to the ATM. They also advise banks and ATM deployers to use technology-based solutions to identify foreign objects being attached to an ATM (also see 3VR Incorporated, 2011:2).

In various counterfeit card fraud cases a collective analysis of positive spend transaction data was used with success to identify CPPs[25]. However, during the docket analysis that was performed by the researcher, it was established that none of the 100 cases analysed was included in a collective CPP analysis.

(c) Surveillance

Once a point of fraudulent spend or point of compromise has been identified, the investigator should focus on identifying perpetrators by using real-time and recorded camera surveillance and physical surveillance, which can be performed by security personnel, the police or police agents, as proposed by Wendorff-Goerge (2007:2-3), Diebold Incorporated (2014a:1; 2014b:1) and the PCI SSC (2013a:16-17) (also see SAPS, 2011b:1-16). Pillay (2011:3) states that the use of real-time camera surveillance from an off-site operational centre and physical observation at ATMs and pay points are effective in identifying points of compromise, suspects and skimming devices by focusing on suspicious behaviour of persons.

Various examples of counterfeit card fraud cases have been found during which police and bank investigators used real-time camera surveillance, recorded surveillance footage and physical observation effectively to identify ATMs and point-of-sale terminals as points of compromise and to identify suspects positively[26]. However, the docket analysis showed that in 82 of the 100 cases studied, SAPS investigating officers did not establish whether any surveillance camera footage of

[25] Including Park Road CAS 880/10/2011, Middelburg MP CAS 309/10/2011, Volksrust CAS 68/04/2013, Malelane CAS 20/09/2013, Crystal Park CAS 206/04/2013 and Sinoville CAS 487/04/2013. In these cases, the accurate identification of common points of compromise was followed up by surveillance activities, which led to the positive identification of perpetrators who were active at the CPPs.

[26] Including Humewood CAS 316/02/2012, Idutywa CAS 11/08/2012, Uitenhage CAS 426/01/2012, Witbank CAS 628/04/2012, Sasolburg CAS 185/08/2013 and Sea Point CAS 284/05/2013.

fraudulent transactions was available at the bank or merchant venue, while in another four (4) cases it was not possible to determine whether any attempts were made to obtain surveillance footage. Actual surveillance camera footage was not used in any of the 100 cases in an attempt to identify suspects.

In terms of SAPS National Instruction 2 of 2013, photographs of all suspects charged for offences listed in Schedule 1 to the Criminal Procedure Act, 1977 (which includes fraud) must be captured on the SAPS National Photographic Image System (NPIS) (SAPS, 2013a). Photographs of suspects captured on the NPIS are linked to personal identifying information which is captured on CAS when a suspect is charged. The Inkwazi database system can also be used to store and retrieve photographs of suspects (SAPS, 2006a:1-3; 2007:1-2). Hence, the NPIS and Inkwazi are sources which can aid counterfeit card fraud investigators to identify unknown suspects from surveillance footage, by comparing their images with photographs of known suspects which already exist on the databases. An investigator can also use photographs from NPIS to generate photo identification parades to identify unknown suspects.

(d) Call data analysis

The analysis of cellphone call data and handset usage profiles of suspects can also be used to identify perpetrators, based on cellphone communications. Schmitz and Cooper (2015:327-332, 336-338), as well as Smith and Zinn (2015:431-432), illustrate that an analysis of account holder information, cellphone and/or landline call data can be used to identify a suspect positively based on RICA information, and to identify a suspect's accomplices, based on outgoing and incoming messages and calls. A call data analysis can also provide evidence of collaboration between suspects and provide a basis to compile an association chart showing linkages between suspects and time lines, illustrating the sequence of events and chronological involvement of suspects in criminal activity.

During investigation, call data, handset usage profiles and account holder information can be obtained from telecommunication service providers in terms of section 205 of the Criminal Procedure Act, 1977. In counterfeit card fraud cases,

cellphones and SIM[27] cards are often seized (see Annexure F as per attached). These should be subjected to a digital forensic analysis, followed by a call data analysis[28] and a handset usage profile analysis in order to identify and link suspects, and to present evidence of collaboration between suspects.

(e) Fingerprint examination and analysis

A fingerprint examination and an analysis of fingerprints retrieved from a counterfeit card, skimming device, PIN-capturing device, card writer or related equipment can be used to identify a suspect positively whose fingerprint profile is on record and/or to link the suspect to the exhibits (National Forensic Science Technology Center, 2009:5-6; Gardner, 2005:26; Marais, 1992:176-181). In the case of Sandton CAS 441/04/2013 it was demonstrated that suspects could be identified positively by means of latent fingerprints, which were recovered from ATM-mounted skimming devices and counterfeit cards (also see Annexure F as per attached). These cases show the importance of subjecting all relevant devices, equipment, components, materials and accessories used by perpetrators to a fingerprint examination.

The transfer of fingerprints to physical objects is based on Locard's exchange principle, which states that with contact between two objects, there will be an exchange of physical evidence (Chisum & Turvey, 2000:3; Minor, 2013:1). Whenever a person comes into contact with an object, crime scene or another person, a cross-transfer of physical matter occurs. With this in mind, it is important to prevent contamination and destruction of latent fingerprints on ATMs, skimming devices, PIN-capturing devices and related equipment. Non-tangible evidence can also be transferred by means of digital (electronic) contact without any physical contact, for example data stored in digital format on a computer or digital storage device, cellphone call data, emails and digital messages (Van Graan & Budhram, 2015:46). Appropriate procedures for the collection, documenting, packaging, preservation and analysis of non-tangible evidence and physical evidence are equally important.

[27] Subscriber Identity Module.
[28] In the cases of Sea Point CAS 284/05/2013, Ermelo CAS 217/02/2012, Amersfoort CAS 87/08/2012, Potchefstroom CAS 298/10/2013 and Beaufort West CAS 525/09/2013, suspects were identified positively and linked to one another by means of cellphone call data analyses.

(f) Profiling of suspects

It has been shown in different counterfeit card fraud cases that the profiling of a known suspect can be used effectively as a method to identify suspects, who had been charged as a co-accused of the known suspect previously[29]. Profiling involves the collating of relevant personal, biographical and criminal information of a suspect (Van Niekerk et al, 2015:213-216), including the suspect's name, surname, date of birth, identity number, photograph, addresses, contact details, spouse, next-of-kin, criminal background, assets and financial information. These should be obtained from all available sources (including SAPS case dockets, investigators, the Crime Administration System, the Criminal Record and Identification System, the Electronic National Administration Traffic Information System (eNatis), the Population Register, Internet sources and credit bureaus). Based on the criminal background of a known suspect, the identity of other suspects can be established from previous criminal cases where they were charged together. A previous co-accused of a known suspect can be profiled and his/her photograph from the NPIS can be used to identify unknown suspects captured on surveillance camera footage.

(g) DNA profiling

DNA profiling (typing) is a process during which deoxyribonucleic acid (DNA) molecules are extracted from a specimen containing genetic material and scientifically analysed, resulting in a unique pattern called a DNA profile, which can be used to identify suspects in criminal cases positively and link them to a crime scene or object (Freckelton & Chambers, 1990:1; De Wet, Oosthuizen & Visser, 2011:3-5). DNA contains a genetic blueprint, which is unique to each individual and can be found in the human body in blood, semen, saliva, soft tissue, bone and skin cells (Manamela et al, 2015:110-115). When the DNA profile originating from physical evidence matches that of a suspect, the latter can be linked positively to the evidence (Goulka, Matthies, Disley & Steinberg, 2010:14; De Wet et al, 2011:3). Different crimes can also be linked based on DNA profiles from evidence found at crime scenes.

[29] Including Queenstown CAS 29/11/2011, Humewood CAS 470/01/2012, Idutywa CAS 11/08/2012, Algoa Park CAS 154/08/2010 and Villieria CAS 43/05/2013.

In South Africa, DNA profiling is recognised by courts as a method to identify a perpetrator positively[30]. DNA profiling has also been used with success in counterfeit card fraud cases to identify suspects positively by means of a positive match with DNA found on skimming devices, counterfeit cards and related equipment[31].

The Criminal Law (Forensic Procedures) Amendment Act, 2013 (Act No. 37 of 2013) deals with DNA sampling and profiling, and maintaining a national forensic database in respect of certain offenders. In terms of this Act, trained police officials have the legal obligation to take a DNA sample from anyone who has been arrested or charged for an offence listed in Schedule 8 of the Criminal Procedure Act, 1977. Fraud and contraventions of the ECT Act and RICA are not included in Schedule 8. However, the SAPS still have legal powers to take DNA samples in counterfeit card fraud and card skimming cases. In terms of the legislation a National Forensic DNA Database (NFDD) will be kept for DNA profiles, consisting of a crime scene index, an arrestee index, a convicted offender index, an investigative index, an elimination index, and an index for missing persons and unidentified human remains.

Goulka et al (2010:15-16) point out that significant success has been achieved with matching crime scene DNA with DNA profiles of known suspects in the United States and the United Kingdom. Odendaal (2014:1) argues that the same measure of success can be achieved in South Africa over time as the number of DNA profiles on the NFDD increases (also see Smith & Zinn, 2015:406). Therefore, a concerted effort should be made by all counterfeit card fraud investigators to collect and submit DNA samples taken from suspects, crime scenes, counterfeit cards, skimming devices, PIN-capturing devices and related equipment for analysis and capturing on the NFDD. This will contribute towards expanding the database and improve chances of future identification of suspects, based on DNA collected from crime scenes and exhibits.

[30] In *S v Nyembe* 2014 (1) SACR 105 (GSJ) the court accepted the positive identification of the accused in three different cases based solely on DNA profiling and analysis. The accused was convicted of 14 counts, including rape, kidnapping, attempted murder and robbery, and was sentenced to life imprisonment.

[31] Including the cases of Nelspruit CAS 206/11/2011, Bethal CAS 68/02/2013, Malelane CAS 20/09/2013 and Witbank CAS 1045/10/2013.

3.2.1.4 Imprint identification in counterfeit card fraud cases

When an object comes into contact with another object, distinctive marks or imprints can be made by one onto the other. Petraco (2011:xv) explains that imprints may depict an object's physical structure through distinctive characteristics, including class characteristics (design and morphological features), manufacturing patterns, wear patterns, damage patterns and microscopic striations. Van Graan and Budhram (2015:51) list various categories of impression evidence, including body prints (fingerprints, palm prints and foot prints), footwear prints, tyre imprints, bite marks, and marks made by power tools, hand tools and firearm mechanisms (also see Marais, 1992:151-186).

Counterfeit cards possess digital impression evidence on a microscopic level in the form of skimmed data, which is encoded magnetically through changes in the alignment of particles in the magnetic strip, using a card writer, computer and appropriate software (Kamal, 2006:2-3). In Annexure F, various cases are cited where digital forensic analyses have been used to provide impression evidence to prove that cards were counterfeit. When an entire card is counterfeited, marks and imprints can be transferred from the equipment used to manufacture the card during the stamping, tipping and embossing processes (Iannacci & Morris, 2000:68-69). Should a counterfeit card be recovered together with the tipper machine and/or embossing machine, imprint identification can be used to positively link the card (and, therefore, the suspect in whose possession it was found) to the relevant equipment[32].

3.2.1.5 Action identification in counterfeit card fraud cases

This category of identification relates to the individualising of human actions as that of a particular offender on the basis of evidence and/or specific methods used (modus operandi) when committing the offence or transgression (Gilbert, 1993:163; Van Graan & Budhram, 2015:52). Modus operandi (method of operating) refers to specific characteristic conduct by a person when committing a crime (Bennett & Hess, 2004:552). It includes aspects such as the behaviour and actions of the offender, the day of the week, the time of the day and location which are chosen to

[32] This type of identification was achieved successfully in the cases of Pretoria West CAS 165/02/2014 and Pretoria Central CAS 1054/02/2014.

commit the crime, the instrument, tool or equipment used, the type of victim and/or property targeted, the type and severity of violence used, unique trademarks and 'signatures' left on a crime scene, and items/objects collected from the crime scene by the offender (also see Van Graan & Budhram, 2015:62 and Labuschagne, 2015:277-279).

Perpetrator identification and action identification are often closely related. A perpetrator can be identified by identifying his/her actions while committing the crime. In Annexure F, various cases have been listed where surveillance of the physical actions and modus operandi of a suspect using a skimming device to skim a card, shoulder surfing to obtain PINs and/or persistently offering unsolicited help to ATM users have led to the identification of the suspects (also see Banking Association of South Africa, 2013:1-2).

Modus operandi in counterfeit card fraud cases also include the build and assembly method, materials, components/parts, accessories and equipment used to manufacture skimming devices and PIN-capturing devices, as well as the methods and equipment used to produce counterfeit cards (SAPS, 2009d:1-3; 2011a:1-5; 2011b:1-12) (see paragraph 2.6). Skimming devices and PIN-capturing devices differ in operation and in levels of sophistication and technological advancement, ranging from very basic to highly advanced (e.g. computer-aided designs, three-dimensional [3-D] printing and transmitting data via cellphone networks, bluetooth or wi-fi) and can provide a good indication of the modus operandi and skills levels of the specific individuals involved (Coyne, 2013:1-3; Feinberg, 2014:1-5). Investigators should be aware of the potential which action identification and modus operandi have to identify perpetrators positively.

3.2.1.6 Cumulative identification in counterfeit card fraud cases

Cumulative identification refers to the collective value of all identification activities that have contributed to identify all relevant aspects positively in order to solve the crime (Lee & Harris, 2000:11). No crime can be solved on the basis of a single category of identification. In order to solve a crime any investigation, no matter how trivial or elementary, requires at least four categories of identification-related activities, being the identification of the crime, the victim, the perpetrator and relevant evidence (Marais, 1992:2-5).

Cumulative identification is illustrated in the appeal *of Ntsele v S* [1998] 3 ALL SA 517 (A), where the trial court had convicted the appellant of several counts of robbery, murder and attempted murder[33]. In counterfeit card fraud cases, the totality of evidence required to establish a cumulative identification will depend on the circumstances of each case and the aspects that need to be identified[34].

3.3 THE SHARING OF INFORMATION AND INTELLIGENCE IN COUNTERFEIT CARD FRAUD CASES

The South African Police Service has a legal obligation to investigate, combat and prevent counterfeit card fraud. To this end, the SAPS has been following an approach of information-sharing in the investigation of banking-related crimes, including counterfeit card fraud (SAPS, 2005:1-4; 2006a:1-3; 2006c:1-4). In terms of SAPS directives all operational information and intelligence relating to banking crime cases must be shared among investigating officers, including biographical profiles and photographs of suspects and accused, descriptions and photographs of skimming devices, PIN-capturing devices and related equipment, modus operandi, bank account numbers, telephone and cellphone numbers, vehicle-related information, addresses, surveillance footage, points of compromise and points of fraudulent spend.

The advantages of information-sharing in counterfeit card fraud cases include the following (SAPS, 2006e:1-3; 2007:1-2; 2011f; Smith & Zinn, 2015:422-430):

- The identification of suspects in a specific geographic area based on, inter alia, surveillance material, offender profiling and modus operandi.
- The real-time availability of photographs, descriptions, profiles and fingerprints of offenders.
- The linking of different offences (cases) committed by the same suspect(s), leading to more charges against suspects, and establishing additional grounds for opposing bail and improving sentences.

[33] Considering the cumulative effect of all the evidence presented, the Supreme Court of Appeal found that it could make no finding other than that the appellant was responsible for committing all the crimes of which he was convicted and the appeal was dismissed.

[34] In the cases of Winterton CAS 21/09/2013 and Malamulele CAS 144/08/2013 cumulative identification was achieved through a series of identification-related activities, including situation, victim, perpetrator, imprint and action identification (also see Annexure F as per attached).

- The solving of cases by positively linking unsolved cases to solved cases on the basis of operational information, thereby improving the detection rate of cases.
- The identification of criminal associates/accomplices and assets of a suspect.
- The identification of crime hotspots through crime pattern and crime threat analyses, and the effective, focused use of personnel, resources and time.
- It promotes a coordinated approach in centralising cases across jurisdictions and contributes towards expediting the finalisation of cases.

The SAPS and Sabric have established and maintained a partnership based on cooperation and mutual assistance in banking crime investigations (SAPS, 2006b:1-3; 2011a; 2011b; 2014:1-6). Sabric (2013c:27; 2015:30) views joint industry and law enforcement investigations as an important tool in the fight against counterfeit card fraud. The foundation for this is the mutual sharing of information and intelligence relating to counterfeit card fraud patterns, tendencies, suspects, crime scenes, hotspots, devices/equipment used and modus operandi. Information-sharing and joint ownership of banking crime databases are among the strategic deliverables of the SAPS(s)abric partnership (SAPS, 2014:2).

Pillay (2011:3) also highlights a close working relationship between Sabric, the SAPS and bank investigators, information-sharing and a central incidence intelligence database as key to investigate counterfeit card fraud effectively. The two Sabric participants mentioned that Sabric provides various information-sharing platforms and tools to enable investigators to identify suspects, points of compromise, points of fraudulent spend, skimming devices, PIN-capturing devices and related equipment. These include a suspect persona database, which contains incidence intelligence, profiles and photographs of suspects, and the dissemination of suspect profiles and case linkage analyses to investigators. Furthermore, Sabric distributes a weekly provincial crime pattern and hotspot analysis (the Tactical Weekly Provincial Commercial Crime Risk Forecast) (see paragraph 3.2.1.3 (a)) and maintains a database for telephone numbers, cellphone numbers and call data. Sabric also provides an online portal where investigators can share information, and

a real-time closed group network (Blue Goose), which is used to inform investigators about arrests and banking crime incidents by means of cellphone messages.

During interviews, participants were asked how Sabric could assist investigators to identify points of compromise, points of fraudulent spend, and patterns and tendencies in respect of counterfeit card fraud. The following responses were received:

- By coordinating investigations between the SAPS and bank investigators, and promoting cooperation, assistance and support from banks (25 participants).
- By providing linkages between cases and suspects (23 participants).
- By maintaining centralised databases, which are accessible for investigators, pertaining to counterfeit card fraud incidents, suspect profiles, devices and equipment used, organised criminal groups, cellphone numbers and call data of perpetrators (19 participants).
- Through assistance to the SAPS in identifying and prioritising perpetrator targets and threats (12 participants).
- By lending support in providing bank transaction analyses to investigators for specific investigations to determine common points of compromise and common points of fraudulent spend (11 participants).
- Through continued support in providing investigators with regular crime information analyses relating to counterfeit card fraud patterns, hotspots and common points of fraudulent spend (10 participants).

It is, therefore, evident that participants in general recognise and agree on the need for the supportive role played by Sabric. Examples of information-sharing and joint investigations involving the SAPS, bank investigators and Sabric, which have led to the positive identification, arrest and conviction of suspects, recovery of counterfeit cards, card skimming and counterfeiting equipment, are listed below[35].

[35] Akasia CAS 500/07/2013, Dunnottar CAS 44/07/2013, Douglasdale CAS 816/05/2013, Sinoville CAS 487/04/2013 and Crystal Park CAS 153/03/2013 (also see Annexure F as per attached).

3.4 SUMMARY

In this chapter, the different categories of identification and specific aspects that require positive identification during counterfeit card fraud investigations were discussed. These aspects include the victim, the negative spend (fraudulent transactions), the positive spend (transactions prior to the fraud), the perpetrators, counterfeit card, skimming device, PIN-capturing device, the point of compromise of the original card (CPP) and point(s) of fraudulent spend (merchant venue(s) and/or ATM(s)).

It was established that counterfeit card fraud cases manifest as different situations and that the aspects which need to be identified, depended on the specific case situation with which the investigator is dealing. An accurate situation identification is, therefore, important in counterfeit card fraud cases.

Different methods to identify the various aspects that need to be identified were examined and it was determined whether these were effective in practice. Perpetrator identification is one of the main pillars upon which a counterfeit card fraud investigation rests. The researcher established that direct and indirect methods could be used to identify perpetrators positively. Different methods of perpetrator identification were discussed. The role and importance of information-sharing and cooperation between SAPS investigators, bank investigators and Sabric, specific to identification in banking-related cases, were also examined.

In the next chapter, the important findings of the study are reported, followed by relevant recommendations.

CHAPTER FOUR:
FINDINGS AND RECOMMENDATIONS

4.1 INTRODUCTION

The incidence of counterfeit card fraud in South Africa is high (Sabric, 2014:1-23; 2015:1-24). However, the identification of offenders who commit these crimes is a serious concern, as police and bank investigators find it difficult to achieve. The result is that the majority of counterfeit card fraud cases reported to the SAPS remain unsolved. One of the reasons for conducting research is the desire to solve a real-life problem. The problem in this study relates to the challenge of identifying the perpetrators of counterfeit card fraud during the investigation of cases.

The aim of this study was to evaluate identification methods used to investigate counterfeit card fraud. The purpose of the study was to explore the topic and the research problem in depth, to examine and evaluate the use of identification methods in counterfeit card fraud investigations, and to empower investigating officers with knowledge on the use of effective identification methods. In order to achieve the research aim and purpose, the following research questions were asked:

- What are the objectives of forensic investigation in counterfeit card fraud investigations?
- What identification methods can be used to investigate counterfeit card fraud?

The research rationale, research problem and research questions were evaluated with the view to make findings and recommendations.

4.2 RESEARCH FINDINGS

The following findings relate to the research questions, and are based on information obtained from the participants as well as relevant national and international sources. Where applicable, the number of participants who have provided specific responses is indicated in brackets.

4.2.1 Research Question One

What are the objectives of forensic investigation in counterfeit card fraud investigations?

The findings in respect of this research question are outlined below.

4.2.1.1 Forensic investigation

Forensic investigation is a process of inquiry into criminal conduct, a civil or administrative matter and involves an in-depth, meticulous search for the truth through the use of specialised skills, expert knowledge, and scientific methods and techniques. Its purpose is to investigate evidence in a scientific manner to establish who committed a crime or transgression and to bring the perpetrator before a court of law or other presiding authority. The main task of a forensic investigator is to identify, collect and present all relevant evidence to enable a presiding officer to establish the truth in respect of an alleged offence or issue under dispute.

Participants in general had a good understanding of what forensic investigation is.

4.2.1.2 Objectives of forensic investigation

The main objectives of forensic investigation are the following:

- The identification of the crime.
- The identification of the perpetrator(s).
- The individualisation of the crime.
- The collecting and processing of evidence and information.
- The evaluation of evidence and information.
- Tracing of the suspect(s) and ensuring court appearances.
- Recovery of property and restitution.
- Support and involvement during the prosecution/litigation phase.
- Victim empowerment.

Participants were generally not able to list all the objectives of forensic investigation.

4.2.1.3 Counterfeit card fraud

Counterfeit card fraud is a specific type of fraud where specific modus operandi and equipment are used to commit the crime. There are three stages in counterfeit card

fraud, collectively referred to as its lifecycle, namely the compromising of a valid bank-issued card at a point of compromise, the manufacturing of a counterfeit card by encoding another card with the skimmed card data, and the actual commission of fraud when the counterfeit card and cardholder's PIN are used to withdraw cash and/or make purchases at a point of fraudulent spend (ATM or merchant venue).

All participants interviewed were able to explain what fraud is and what the elements of fraud are. Participants in general had an understanding of how counterfeit card fraud is committed, as well as the different types of card skimming and PIN capturing. However, nine (9) participants did not know how POS skimming was committed. Fourteen (14) investigators indicated that they have investigated all three types of skimming. Ten (10) investigators have investigated only handheld skimming and ATM skimming, while three (3) have investigated only handheld skimming.

4.2.1.4 Card skimming

Card skimming is performed by using any of three methods, namely handheld skimming, ATM skimming or point-of-sale skimming. PIN capturing is done with a miniature (pinhole) camera, a pinpad overlay, an altered POS device or by surreptitiously observing the cardholder when entering the PIN on a pinpad (shoulder surfing).

4.2.1.5 SAPS training with regard to counterfeit card fraud

Investigation-related courses presented to SAPS investigators include the Basic Crime Investigation Course, Resolving of Crime Course and the Commercial Crime Forensic Learning Programme Levels I, II and III. However, none of these address the objectives of identification and individualisation in counterfeit card fraud. SAPS investigators are not formally trained on how to use effective identification methods in the investigation of counterfeit card fraud.

4.2.2 Research Question Two

What identification methods can be used to investigate counterfeit card fraud?

The following findings were made in respect of this research question:

4.2.2.1 Identification

Identification is a process of classification by which an entity, person or object is placed in a predefined class or category, based on shared or similar features or characteristics (class characteristics). Identification forms the basis for individualisation, which relates to a unique (positive) identification.

4.2.2.2 Categories of identification

Identification can be divided into seven (7) primary categories, namely:

- Victim identification.
- Witness identification.
- Perpetrator (culprit) identification.
- Imprint identification.
- Origin identification.
- Action identification.
- Cumulative identification.

4.2.2.3 Aspects for identification in counterfeit card fraud cases

Depending on the specific circumstances of a case, there are several aspects which require positive identification during counterfeit card fraud investigations. These aspects include the following:

- The modus operandi, type of skimming, skimming device and PIN-capturing device used (26 participants).
- The person who used the skimming device and PIN-capturing device to illegally obtain the card and PIN data (25 participants).
- The person(s) who performed the fraudulent transactions (25 participants).
- The point(s) of fraudulent spend (merchant(s) and/or ATM(s)) (24 participants).
- The point of compromise of the original card or a common point of compromise of various compromised cards (common point of purchase) (23 participants).
- The person who manufactured the counterfeit card(s) (22 participants).

- The place where the counterfeit card(s) was/were produced (19 participants).
- The equipment used to manufacture the counterfeit card(s), including the card encoder, computer equipment and, where applicable, card embosser and tipper (18 participants).
- The counterfeit card(s) which was/were used (18 participants).
- The fraudulent (disputed) transactions (fraudulent/negative spend) (18 participants).
- The specific point-of-sale terminal and cashier at a merchant venue where the counterfeit card was presented (16 participants).
- The person who supplied or manufactured the skimming device and PIN-capturing device (16 participants).
- The cellphone numbers of perpetrators and their communications with each other (16 participants).
- The equipment and materials used to manufacture the skimming device and PIN-capturing device (14 participants).
- The place where the skimming device and PIN-capturing device were manufactured (14 participants).
- The prior to fraud transaction history (positive spend) (12 participants).
- The crime (identifying the crime as counterfeit card fraud) (10 participants).
- Any other person who colluded to commit the crime, including those who shared in the proceeds (6 participants).

4.2.2.4 Victim identification

In order to identify unknown victims in counterfeit card fraud cases, an investigator can make use of the following methods:

- A digital forensic analysis of counterfeit cards, skimming devices and/or related equipment which are recovered (20 participants).
- With information and the assistance of the bank (18 participants).
- An analysis of merchant transaction vouchers and/or the ATM electronic transaction journal (8 participants).

4.2.2.5 Perpetrator identification

It was established that the following methods can be used to identify perpetrators in counterfeit card fraud cases positively:

- Identifying common points of fraudulent spend, supported by surveillance to identify previously known fraudsters and suspects acting suspiciously (e.g. making multiple withdrawals using different cards, withdrawing money around midnight or obscuring their faces from surveillance cameras) (16 participants).
- Identifying a common point of compromise of different cards, which have been compromised in the same geographical area over the same period, supported by surveillance to identify previously known suspects and suspects behaving suspiciously (including card skimming, shoulder surfing, loitering in the vicinity of an ATM or persistently offering unsolicited help to others) (16 participants).
- The purposeful surveillance of popular and frequently used ATMs and merchant venues in order to identify previously known suspects, as well as suspicious actions related to card skimming and PIN capturing (15 participants).
- A thorough interview of all suspects arrested and obtaining information in order to identify other suspects (15 participants).
- Call data and cellphone handset usage analysis of suspects in order to identify accomplices by means of contact details and communications (13 participants).
- Fingerprint examination and analysis in respect of recovered counterfeit cards, skimming and PIN-capturing devices, false panels and overlays, components and related equipment in order to identify suspects from existing criminal databases (10 participants).
- DNA profiling (3 participants).
- Profiling of suspects (2 participants).

4.2.2.6 Identifying points of fraudulent spend

The following methods to identify points of fraudulent spend were established during research:

- An interview with the victim during which negative spend (fraudulent transactions) should be identified from relevant bank statements. Information identifying the specific point(s) of fraudulent spend (merchant or ATM) should be obtained from the bank statements. Should the bank statements be inadequate to identify the point(s), additional information must be obtained from the bank (19 participants).
- Surveillance of suspected points of fraudulent spend in order to identify suspects behaving suspiciously (e.g. making multiple withdrawals using different cards at the same ATM, making withdrawals at midnight or obscuring their faces from surveillance cameras) (16 participants).
- A collective analysis of negative (fraudulent) spend transaction data relating to different cards which have been compromised in the same geographical area over the same period (12 participants). Sources, tools and aids which can be used to perform such an analysis, include bank statements, Microsoft Excel spreadsheets, i2 Analyst's Notebook and Sabric analysts.
- The thorough interviewing of suspects in custody in order to identify points of fraudulent spend (10 participants).
- Identifying common points of fraudulent spend (fraud hotspots) from the Tactical Weekly Provincial Commercial Crime Risk Forecast, which is compiled by Sabric and distributed to SAPS and bank investigators (see Annexure G) (7 participants).
- A crime information analysis in respect of counterfeit card fraud cases reported to the SAPS (which should include a crime pattern analysis, an analysis of modus operandi, identifying and mapping hotspots), using data sources, tools and techniques available in the SAPS (Crime Administration System, Geographic Information System, Microsoft Excel spreadsheets, i2 Analyst's Notebook, i2 iXa and iXv Visualiser). Crime information analyses could also be obtained from the station crime information official (2 participants).

The docket analysis which was performed during research, showed that in only 28 of the 100 cases analysed the point of fraudulent spend was identified positively. This meant that in 72 cases SAPS investigators never established where the criminals

had used the counterfeit cards. This could be a contributing factor as to why, in the majority of counterfeit card fraud cases, perpetrators are not identified positively and the crimes are never individualised.

4.2.2.7 Identifying common points of compromise

The following methods to identify common points of compromise (CPPs) effectively can be used:

- An interview with the victim during which positive spend (legitimate transactions prior to fraudulent transactions) should be identified from relevant bank statements (18 participants). The process is similar to that of identifying the point of fraudulent spend; however, here positive spend data is used. During the interview, attempts should be made to identify possible points of compromise.
- Surveillance of suspected points of compromise in order to identify suspects behaving suspiciously (e.g. performing card skimming and/or PIN-capturing activities, persistently offering unsolicited help to cardholders, obscuring their faces from surveillance cameras and/or loitering in the vicinity of an ATM) (16 participants).
- A collective analysis of positive spend transaction data relating to different cards which have been compromised in the same geographical area over the same period, based on victims' bank statements. The same tools and aids which are used to identify common points of fraudulent spend, apply here (11 participants).
- A thorough interview of suspects in custody in order to identify points of compromise (10 participants).

The docket analysis showed that in none of the 100 cases analysed a CPP analysis was done.

4.2.2.8 Surveillance

Surveillance of points of fraudulent spend and points of compromise offer investigators the opportunity to identify perpetrators of counterfeit card fraud. Surveillance should include real-time and recorded camera surveillance as well as physical surveillance, which can be performed by security personnel, the police or

police agents. Photographs of known fraudsters can be obtained from the National Photographic Image System and Inkwazi System of the SAPS. These can be used to identify unknown suspects who have been captured on surveillance footage.

During the docket analysis it was found that in 82 of the 100 SAPS cases, investigating officers did not establish whether any surveillance footage of the fraudulent transactions was available. Surveillance footage was not used in any of the cases in attempt to identify suspects. This may also be a factor which has contributed to the low rate of identifying perpetrators of counterfeit card fraud positively.

4.2.2.9 Imprint identification

Imprint identification in counterfeit card fraud cases can be achieved by subjecting recovered counterfeit cards, skimming devices, PIN-capturing devices and related equipment to a digital forensic analysis in order obtain evidence of, and to retrieve skimmed card and PIN data. Physical marks made onto a counterfeit card by a tipping machine or embossing machine can also be identified by an appropriate forensic expert. Hence, based on physical impression evidence, a counterfeit card can be positively linked to the specific equipment which was used to manufacture it.

4.2.2.10 Action identification

Action identification in counterfeit card fraud cases can be achieved by identifying suspicious behaviour of perpetrators, including card skimming and PIN-capturing activities, the use of a counterfeit card, ATM withdrawals made at midnight, obscuring his/her face from surveillance cameras, loitering at an ATM and/or persistently offering unsolicited help to ATM users. Modus operandi, in particular the build and assembly method and technological sophistication of skimming devices and PIN-capturing devices, can also guide an investigator to identify the correct perpetrator.

4.2.2.11 The sharing of information and intelligence

The sharing of incidence information and intelligence and a coordinated approach by relevant role players, including the SAPS, banks and Sabric, create an environment which enable investigators to identify perpetrators of counterfeit card fraud.

4.3 SECONDARY FINDINGS

The researcher also made a number of secondary findings with regard to relevant points during the research.

4.3.1 Debit card

A debit card is a payment instrument which is issued by a financial institution and linked to a deposit account (e.g. a cheque, savings or transmission account) which, generally, is pre-funded and has a lower credit risk exposure than a credit card.

4.3.2 Credit card

A credit card is a payment instrument which is issued by a financial institution and linked to a credit card account with a pre-approved credit limit, which enables the cardholder to purchase goods and services from merchants who have agreed to accept the card.

4.3.3 Responsibility, mandate and powers to investigate

In South Africa, investigators can be divided into two categories, namely SAPS investigators and non-SAPS investigators. Non-SAPS investigators include government departments and agencies, as well as private entities with investigative capacity, including bank, corporate and private investigators. In terms of legislation the South African Police Service is the primary institution responsible for the investigation of crime.

4.3.4 Evidence

Evidence is anything with evidential (probative) or exculpatory value that is relevant to a case. It can be used to prove or refute (disprove) a fact or allegation and includes, but is not limited to, physical objects, documents, information and witness testimony.

4.3.5 Locard’s exchange principle

Locard’s exchange principle holds that, whenever two objects come into contact, there will be a cross-transfer of physical matter between them. A perpetrator who physically touches an object on a crime scene will leave traces of physical evidence, which may include fingerprints and/or DNA material. Non-tangible evidence can also be transferred by means of digital (electronic) contact without any physical contact;

for example, data stored on a computer, cellphone call data, e-mails and digital messages.

4.3.6 Manifestations of counterfeit card fraud

Counterfeit card fraud cases manifest as any of the following situations or a combination of two or more:

- A complaint from a cardholder who has suffered a loss on his/her bank account has been received by the bank or SAPS (in these cases the suspect, the method of skimming and point of compromise of the card are usually unknown).
- Information relating to card skimming and/or counterfeit card fraud activities has been received or collected by the bank or SAPS.
- A counterfeit card, skimming device and/or PIN-capturing device has/have been recovered.
- A suspect has been arrested on suspicion of card skimming and/or counterfeit card fraud.

During interviews, 26 of the 29 participants (who included both Sabric participants) mentioned complaints from cardholders who suffered losses on their accounts, where the perpetrator(s), method of skimming and point of compromise are unknown, as the most common manifestation of counterfeit card fraud.

4.3.7 Situation identification

Situation identification involves an evaluation of the circumstances and evidence found by the investigator in a specific situation. Based on the investigator's observations, investigative knowledge and experience, an inference can be made as to whether an incident has taken place or a crime has been committed. An accurate situation identification is only possible if the investigator has a sound knowledge of the crime and the required elements of the crime, supported by practical experience of crime scenes and situations. In order to achieve an accurate situation identification in counterfeit card fraud cases, the investigator should conduct a thorough interview with the victim.

4.4 RECOMMENDATIONS

The research has focused on the subject of identification methods in the investigation of counterfeit card fraud cases. A number of the findings from the docket analysis and interviews with investigators clearly reflect the absence of effective identification methods during investigations. The research has been an attempt to find out what good practices exist for effectively identifying the various aspects that need to be identified during counterfeit card fraud investigations and, in addition, to equip investigators with new knowledge in that respect. Without recommendations on how to improve the identification efforts of investigators, the research would be fruitless and of no meaning. Keeping in mind the salient findings of the research, the researcher makes the following recommendations:

4.4.1 Research Question One

It is recommended that:

- The objectives of forensic investigation in counterfeit card fraud cases specific to identification and individualisation be included in the formal training curricula for SAPS investigators. The existing training material should be revised to address these objectives.
- SAPS and bank investigators be trained in respect of point-of-sale skimming and how to investigate it.

4.4.2 Research Question Two

The following recommendations are made:

- A training manual should be developed by relevant role players, including the SAPS, the banks and Sabric, relating to the most effective identification methods which can be used to positively identify different aspects in different case settings in counterfeit card fraud cases. It is also recommended that training be expedited by means of workshops, joint forums, mentorship programmes and on-the-job training.
- Sabric and bank investigators should be used as resources by SAPS investigators on a regular basis to assist with identification during counterfeit card fraud investigations, in particular to identify common points of fraudulent spend, common points of compromise and perpetrators.

- The Tactical Weekly Provincial Commercial Crime Forecast issued by Sabric should be used by SAPS and bank investigators as a guideline to identify common points of fraudulent spend. Investigators should place these points under surveillance or use available surveillance footage and incidence intelligence. SAPS and bank investigators should focus their resources, time and efforts towards identifying perpetrators active at identified points.
- Counterfeit card fraud investigators should analyse positive spend and negative spend transaction data to identify points of compromise and points of fraudulent spend, respectively, by using available sources, tools and techniques, including CAS, GIS, case dockets, bank statements, Microsoft Excel spreadsheets and Analyst's Notebook software.
- SAPS counterfeit card fraud investigators should use station-level crime information officials to assist with crime information analyses, crime patterns and crime mapping in respect of counterfeit card fraud incidents reported to the SAPS.
- Counterfeit card fraud investigators should employ perpetrator identification methods which are underutilised, including recorded surveillance footage, fingerprint examination and analysis, and DNA examination and analysis.
- A fingerprint examination and analysis should be compulsory in all cases where counterfeit card fraud-related devices, equipment and/or materials are seized.
- SAPS counterfeit card fraud investigators should be trained to take DNA samples. The taking of DNA samples from suspects who have been arrested for counterfeit card fraud and/or card skimming, and submission thereof to the National Forensic DNA Database, should be compulsory.
- In order to promote effective identification-related activities during investigations, a check-list should be introduced for use in counterfeit card fraud dockets as a guide to investigators. The completion of the check-list, with specific details of identification-related activities performed by the investigator, should be compulsory.

- The SAPS should take appropriate preventive action in respect of counterfeit card fraud and card skimming, which should include regular awareness campaigns involving the banks and the public.

In addition, it is recommended that further research be conducted on the topic of identification methods in counterfeit card fraud investigations. The researcher believes that it is necessary to study international methods and practices in this regard in more depth. It is important to improve and enhance identification methods used in South Africa with effective international practices.

4.5 CONCLUSION

Technological advancement has created whole new worlds of opportunity for criminals. Digital and computer technology have changed the lives of modern man forever. The skimming and counterfeiting of bank cards is a worldwide phenomenon, which has a huge impact on economies. It is a committed with the aid of advanced technology and offers anonymity, low risk and a high return to criminals. Furthermore, it is complex and difficult to investigate. Investigators are not always skilled and equipped to investigate this type of technologically sophisticated crime. Banks are sometimes not in a position to provide information needed by the investigator or analyst for identification purposes. The reality is that investigators dealing with counterfeit card fraud face serious challenges.

The research has shown that, although effective identification methods exist, investigators often do not apply them and, therefore, offenders are seldom identified during investigation. This is especially true in cases where a victim has reported a loss on his/her bank account, but the suspect, type of skimming and the point of compromise are unknown. Suspects often remain unidentified and cases are closed as undetected. Investigators should realise that there are identification methods that can be used effectively and that they should apply them.

It is a misconception to think that counterfeit card fraud will disappear once chip-and-pin technology has been fully implemented. South Africa is largely chip-and-pin (EMV) compliant but still experiences high levels of counterfeit card fraud (Sabric, 2015:1-5). As there are still large parts of the world which are not EMV compliant (including the United States and parts of Asia), banks and payment card providers

have retained magnetic stripes on cards (EMVCo, 2015). Magnetic stripe-based authentication is still allowed in many EMV compliant countries (Diebold Incorporated, 2011:3). Furthermore, a chip-and-pin card will use magnetic stripe-based authentication if the chip is not functioning. For these reasons card skimming and counterfeit card fraud will continue for years to come.

It can be argued that effective identification and the prevention of counterfeit card fraud go hand-in-hand. Every arrest and conviction has to be preceded by a positive perpetrator identification. Every time a perpetrator is arrested, a skimming device or counterfeit card is seized, a potential fraud is prevented. Counterfeit card fraud typically takes place in an environment which offers opportunities for identification to the investigator, including the security features of cards, bank and card processing systems, the ATM and point-of-sale terminal, the people, procedures and technologies involved. Investigators must look for these opportunities and use them to solve cases.

The researcher believes that this research will empower SAPS investigators with knowledge in respect of identification methods which can be used in counterfeit card fraud investigations, and that it will open up avenues for further research to address the research problem.

LIST OF REFERENCES

Ablett, J. 2014. *6 ATM anti-fraud steps for small FIs.* Available at: http://www.atmmarketplace.com/articles/6-atm-anti-fraud-steps-for-small-fis/ (accessed on: 29 September 2014).

Adams, F., Caddell, A.G. & Krutsinger, J.L. 2004. *Crime scene investigation.* (2nd edn.). New Jersey: Pearson Education.

American Institute of CPAs. [Sa]. *Conducting effective interviews.* Available at: http://www.aicpa.org/ (accessed on: 14 October 2015).

Badenhorst, C. 2007. *Research writing. Breaking the barriers*. Pretoria: Van Schaik.

Baker, S.E. & Edwards, R. 2012. (Eds). *How many qualitative interviews is enough?* Available at: http://eprints.ncrm.ac.uk/2273/4/how_many_interviews.pdf (accessed on: 18 July 2013).

Banking Association of South Africa. 2013. *Card skimming theft.* Available at: http://www.banking.org.za/consumer-information/ (accessed on: 23 October 2014).

Becker, R.F. 2009. *Criminal investigation*. (3rd edn.). Sudbury, MA: Jones & Bartlett.

Becker, R.F. & Dutelle, A.W. 2013. *Criminal investigation*. (4th edn.). Burlington, MA: Jones & Bartlett.

Bennett, W.W. & Hess, K.M. 2004. *Criminal investigation.* (7th edn.). Belmont, CA: Thomson Wadsworth.

Benson, B.C., Jones, G. & Horne, J.S. 2015. Forensic investigation of crime, irregularities and transgressions (Pp. 1-42). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Blandford, A. 2013. Semi-structured qualitative studies (Pp. 1-53). In M. Soegaard & R.F. Dam (Eds). *The Encyclopedia of Human-Computer Interaction.* (2nd edn.). Aarhus: Denmark. Available at: http://discovery.ucl.ac.uk/1436174/2/ semi-structured_ qualitative_studies.pdf (accessed on: 28 November 2014).

Boeije, H. 2010. *Analysis in qualitative research.* London: Sage.

Bouma, G.D. & Ling, R. 2010. *The research process.* (5th edn.). Melbourne: Oxford.

Breuer, A., Hursey, J.J., Stroman, T. & Verma, A. 2008. *Visualization of criminal activity in an urban population*. Available at: http://josh.hursey.me/papers/ 2008/breuer-igi-2008.pdf (accessed on 11 March 2013).

Bryman, A. 2012. *Social research methods.* (4th edn.). Oxford: Oxford University Press.

Burchell, J. 2005. *Principles of Criminal Law*. (3rd edn.). Lansdowne: Juta & Co.

CashCard. 2012. *Your responsibility as a CashCard ATM merchant*. Available at: https://www.cashcard.com.au/content/dam/cashcard/ (accessed on: 27 June 2014).

Champod, C. 2015. Overview and meaning of identification/individualization (Pp. 95-103). In M.M. Houck. (Ed.). *Professional Issues in Forensic Science.* Oxford: Academic Press.

Chisum, W.J. & Turvey, BE. 2000. Evidence dynamics: Locard's exchange principle and crime reconstruction. *Journal of Behavioral Profiling*, 1(1). Available at: http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html (accessed on: 24 June 2014).

Chisum, W.J. & Turvey, B.E. 2011. *Crime reconstruction.* (2nd edn.). Waltham, MA: Academic Press.

Coyne, A. 2013. *Criminals use 3-D printed skimming devices on Sydney ATMs.* Available at: http://www.itnews.com.au/news/criminals-use-3d-printed-skimming-devices-on-sydney-atms-353590 (accessed on: 21 September 2014).

Creswell, J.W. 2009. *Research design. Qualitative, quantitative and mixed methods approaches.* (3rd edn.). Thousand Oaks, CA: Sage.

Creswell, J.W. 2013. *Qualitative inquiry & research design. Choosing among five approaches.* (3rd edn.). Thousand Oaks, CA: Sage.

Dantzker, M.L. & Hunter, R.D. 2012. *Research methods for Criminology and Criminal Justice*. (3rd edn.). Sudbury, MA: Jones & Bartlett.

Denscombe, M. 2002. *Ground rules for good research: A 10-point guide for social researchers*. Philadelphia: Open University Press.

Denscombe, M. 2010. *Ground rules for social research. Guidelines for good practice.* (2nd edn.). Berkshire: Open University Press/ McGraw-Hill.

Detica. 2010. *Common point of purchase compromises: The evolution of the fraudster.* Available at: www.deticanetreveal.com (accessed on: 22 June 2013).

De Wet, S., Oosthuizen, H. & Visser, J. 2011. DNA profiling and the law in South Africa. *Potchefstroom Electronic Law Journal,* 14(4):171-207. Available at: http://www.scielo.org.za/ (accessed on: 24 June 2014).

Diebold Incorporated. 2011. *Battling card fraud through chip and pin technology.* Available at: www.diebold.com (accessed on: 12 May 2013).

Diebold Incorporated. 2014a. *ATM security alert. Skimming device and false enclosure with camera discovered on ATM in Colombia.* E-mail from the Diebold ATM Security Communication and Support Center. 29 August.

Diebold Incorporated. 2014b. *ATM is target of internal skimming attack in New Jersey.* E-mail from the Diebold ATM Security Communication and Support Center. 20 November.

Divitt, D. 2013. *The lifecycle of a fraud.* Available at: www.atmmarketplace.com (accessed on: 25 October 2013).

Dutelle, A.W. 2011. *An introduction to crime scene investigation*. Sudbury, MA: Jones & Bartlett.

Easton, V.J. & McColl, J.H. [Sa]. *Statistics glossary.* Available at: http://www.stats.gla.ac.uk(s)teps/glossary(s)ampling.html (accessed on: 22 May 2013).

EMVCo. 2015. *Worldwide EMV deployment statistics.* Available at: https://www.emvco.com/about_emvco.aspx?id=202 (accessed on: 28 September 2015).

Esker, F. 2013. *Bank fraud protection: Staying one step ahead of the fraudsters.* Available at: www.atmmarketplace.com (accessed on: 20 November 2013).

Europol. 2012. *Situation report - Payment card fraud 2012.* Available at: https://www.europol.eu(s)ites/default/files/1public_full_20_sept.pdf (accessed on: 12 June 2013).

Feinberg, A. 2014. *The evolution of ATM skimmers.* Available at: http://gizmodo.com/the-terrifying-evolution-of-atm-skimmers-1626794130 (accessed on: 11 November 2014).

Ferreira, G. 2012. *Counterfeit card fraud: Is there a need to introduce legislation to facilitate the prosecution of related criminal activities?* Unpublished LLM Dissertation, University of Johannesburg, Johannesburg.

Fisher, B.A.J. 2004. *Techniques of crime scene investigation*. (7th edn.). Washington D.C.: CRC Press.

Forman, G.H. 2005. *Determining point-of-compromise.* Available at: http://www.freepatentsonline.com/y2005/0055373.html (accessed on: 21 May 2013).

Freckelton, I. & Chambers, O.D. 1990. *DNA profiling: Forensic science under the microscope.* Available at: http://aic.gov.au/media_library/publications/proceedings/02/freckelton.pdf (accessed on: 24 June 2014).

Gardner, R.M. 2005. *Practical crime scene processing and investigation.* Washington D.C.: CRC Press.

Gardner, R.M. 2012. *Practical crime scene processing and investigation.* (2nd edn.). Boca Raton, FL: CRC Press/ Taylor & Francis Group.

Giacalone, J.L. 2015. *Four basic steps in a fraud investigation.* Available at: http://blogs.lexisnexis.com/public-safety/2015/06/fraud-investigation-basic-steps/ (accessed on: 12 October 2015).

Gilbert, J.N. 1993. *Criminal investigation*. (3rd edn.). New York: MacMillan.

Given, L.M. (Ed.). 2008. *The Sage encyclopedia of qualitative research methods.* Thousand Oaks, CA: Sage.

Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report,* 8(4):597-606. Available at: http://www.nova.edu(s)sss/QR/QR8-4/golafshani.pdf (accessed on: 18 May 2013).

Goulka, J., Matthies, C., Disley, E. & Steinberg, P. 2010. *Toward a comparison of DNA profiling and databases in the United States and England.* Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2010/RAND_TR918.pdf (accessed on: 25 June 2014).

Gray, D.E. 2014. *Doing research in the real world.* (3rd edn.). London: Sage.

Grix, J. 2010. *The foundations of research*. (2nd edn.). Hampshire: Palgrave Macmillan.

Hayes, D.R. 2014. *Skimming the surface. How skimmer fraud has become a global epidemic.* New York: Pace University.

Heuker, C. 2013. Smart, informed response required to combat skimming. *Banking Automation Bulletin, 3*12:6-7. Available at: https://tmdsecurity.com/UserFiles/File/TMD%20RBR%20Bulletin052013.PDF (accessed on: 13 November 2013).

Hill, B. & Paynich, R. 2014. *Fundamentals of crime mapping.* Burlington, MA: Jones & Bartlett.

Iannacci, J. & Morris, R. 2000. *Access device fraud and related financial crimes.* Boca Raton, FL: CRC Press.

Jordaan, J. 2015. Digital forensic and cybercrime (Pp. 361-396). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Kamal, S.E.S. 2006. The magnetic stripe technology. *Illumin,* VIII(II). Available at: http://illumin.usc.edu/printer/157/the-magnetic-stripe-technology/ (accessed on: 10 September 2014).

Karagiozis, M.F. & Sgaglio, R. 2005. *Forensic investigation handbook.* Springfield, IL: Charles C Thomas.

Kaye, D.H. 2009. Identification, individualization, uniqueness. *Law, Probability & Risk,* 8(2): 85-94. Available at: http:/(s)srn.com/abstract=1425864 (accessed on: 11 June 2013).

Krebs, B. 2010a. *ATM skimmers, Part II.* Available at: http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/ (accessed on: 1 November 2013).

Krebs, B. 2010b. *ATM skimmers: Separating cruft from craft.* Available at: http://krebsonsecurity.com/2010/06/atm-skimmers-separating-cruft-from-craft/ (accessed on: 1 November 2013).

Krebs, B. 2011a. *Point-of-sale skimmers: Robbed at the register.* Available at: http://krebsonsecurity.com/2011/05/point-of-sale-skimmers-robbed-at-the-register/ (accessed on: 2 November 2013).

Krebs, B. 2011b. *Green skimmers skimming green.* Available at: http://krebsonsecurity.com/2011/03/green-skimmers-skimming-green/ (accessed on: 2 November 2013).

Krebs, B. 2012. *Point-of-sale skimmers: No charge … yet.* Available at: http://krebsonsecurity.com/2012/12/point-of-sale-skimmers-no-charge-yet/ (accessed on 2 November 2013).

Krebs, B. 2013a. *Pro-grade point-of-sale skimmer.* Available at: http://krebsonsecurity.com/2013/02/pro-grade-point-of-sale-skimmer/ (accessed on: 2 November 2013).

Krebs, B. 2013b. *Nordstrom finds cash register skimmers.* Available at: http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/ (accessed on: 2 November 2013).

Krebs, B. 2015. *Tracking a bluetooth skimmer gang in Mexico.* Available at: http://krebsonsecurity.com/2015/09/tracking-a-bluetooth-skimmer-gang-in-mexico/ (accessed on: 22 October 2015).

Labuschagne, G. 2015. Criminal investigative analysis: An applied perspective (Pp. 275-304). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Lee, H.C. & Harris, H.A. 2000. *Physical evidence in forensic science*. Tucson: Lawyers & Judges.

Lee, H.C., Palmbach, T. & Miller, M.T. 2003. *Crime scene handbook*. London: Academic.

Leedy, P.D. & Ormrod, J.E. 2013. *Practical research. Planning and design*. (10th edn.). Upper Saddle River, NJ: Pearson.

Levine, J.L. 1996. *Introduction to data analysis: The rules of evidence.* Available at: http://www.dartmouth.edu/~mss/data%20analysis/ (accessed on: 14 March 2013).

Manamela, M.S., Smith, J.H. & Mokwena, R.J. 2015. Serological evidence and DNA analysis (Pp. 95-119). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Marais, C.W. (Ed.). 1992. *Fisiese getuienis in misdaadondersoek.* Pretoria: Henmar.

Maree, K. (Ed.). 2012. *First steps in research.* Pretoria: Van Schaik.

Mason, M. 2010. Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, 11(3):1-19. Available at: http://www.qualitative-research.net/index.php/fqs/article/view/1428 (accessed on: 19 July 2013).

MasterCard International. 2009. *Understanding terminal manipulation at the point of sale.* Available at: http://www.mastercard.com/us/company/en/docs/ (accessed on: 23 October 2013).

MasterCard International. 2010a. *MasterCard expert monitoring solutions fraud scoring.* Available at: www.mastercard.com (accessed on: 14 July 2013).

MasterCard International. 2010b. *How the past changes the future of fraud.* Available at: www.mastercard.com (accessed on: 14 July 2013).

MasterCard International. 2015. *Protecting payments.* Available at: http://www.mastercard.com/uk/merchant/en(s)ecurity/protection/payments (accessed on: 25 March 2015).

MasterCard South Africa. 2009. *MasterCard card identification features.* Available at: http://www.mastercard.com/za/merchant/en(s)ecurity/datasecurityrules/ (accessed on:23 May 2014).

Maxfield, M.G. & Babbie, E.R. 2012. *Basics of research methods for Criminal Justice and Criminology.* (3rd edn.). Belmont, CA: Wadsworth/ Cengage.

Maxwell, J.A. 2005. *Qualitative research design. An interactive approach.* (2nd edn.). Thousand Oaks, CA: Sage.

Minor, J. 2013. *Touch DNA: From the crime scene to the crime laboratory.* Available at: http://www.forensicmag.com/articles/2013/04/touch-dna-crime-scene-crime-laboratory (accessed on 24 June 2014).

Monckton-Smith, J., Adams, T., Hart, A.G. & Webb, J. 2013. *Introducing forensic and criminal investigation*. London: Sage.

Morrow, S.L. 2005. Quality and trustworthiness in qualitative research in counseling psychology. *Journal of Counseling Psychology*, 52(2):250-260. Available at: http://www.safranlab.net/uploads/7/6/4/6/7646935/quality__trustworthiness_2005.pdf (accessed on: 24 October 2014).

Mouton, J. 2008. *How to succeed in your master's & doctoral studies. A South African guide and resource book.* Pretoria: Van Schaik.

National Forensic Science Technology Center. 2009. *A simplified guide to fingerprint analysis*. Available at: http://www.crime-scene-investigator.net/ (accessed on: 11 November 2015).

Nickell, J. & Fischer, J.F. 1999. *Crime science. Methods of forensic detection.* Lexington, KY: University Press of Kentucky.

Noak, I. & Wincup, E. 2004. *Criminological research: Understanding qualitative methods*. London: Sage.

Noble, H. & & Smith, J. 2015. Issues of validity and reliability in qualitative research. *EvidBased Nurs*, 18(2):34-35. Available at: http://ebn.bmj.com/content/18/2/34.full.pdf (accessed on: 18 August 2015).

Odendaal, N. 2014. *DNA Act a monumental step forward for SA.* Available at: http://www.engineeringnews.co.za/article/dna-act-a-monumental-step-forward-for-sa-2014-02-13 (accessed on: 25 June 2014).

Orthmann, C.H. & Hess, K.M. 2013. *Criminal investigation.* (10th edn.). Delmar, NY: Cengage.

Osterburg, J.W. & Ward, R.H. 2010. C*riminal investigation. A method for reconstructing the past.* (6th edn.). New Providence, NJ: Matthew Bender/ LexisNexis.

Oxford Dictionary. 2014. Available at: http://www.oxforddictionaries.com/ (accessed on: 12 April 2014).

PASA – see Payments Association of South Africa.

Payment Card Industry Security Standards Council. 2009. *Information supplement: Skimming prevention – best practices for merchants. PIN transaction program requirements and PCI Data Security Standard (PCI DSS).* Available at: https://www.pcisecuritystandards.org/documents(s)kimming_prevention_IS.pdf(accessed on: 13 May 2013).

Payment Card Industry Security Standards Council. 2013a. *PCI PIN transaction security point of interaction security requirements. Information supplement: ATM security guidelines.* Available at: https://www.pcisecuritystandards.org (accessed on: 21 May 2014).

Payment Card Industry Security Standards Council. 2013b. *Payment Card Industry (PCI) data security standard. Requirements and security assessment procedures.* Available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf (accessed on: 12 April 2014).

Payments Association of South Africa. 2012a. Annual Report 2011.

Payments Association of South Africa. 2012b. *Card-based payment systems.* Available at: http://www.pasa.org.za/more_cardbased.html (accessed on: 20 April 2013).

Petraco, N. 2011. *Color atlas of forensic toolmark identification.* Boca Raton, FL: CRC Press.

PCI SSC – see Payment Card Industry Security Standards Council.

Pillay, R. 2011. Case study ATM fraud. An issuer's perspective. *Security Matters*, 2011:2-3. Available at: https://www.mastercard.com/us/wce/PDF/PSI_ Magazine_ SecurityMatters (accessed on: 22 August 2014).

Rowsell, J. 2013. *Reducing debit card fraud losses: Pinpoint compromised cards through ID of common points of compromise.* Available at: http://www.cuinsight.com (accessed on: 22 April 2014).

Sabric. See South African Banking Risk Information Centre.

SAPS - See South African Police Service.

Savin-Baden, M. & Major, C.H. 2013. *Qualitative research. The essential guide to theory and practice.* Oxon, UK: Routledge.

Schmitz, P.M.U. & Cooper, A.K. 2015. Forensic geography (Pp. 305-357). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Schulz, M. & Ruse, A. 2012. *Credit cards around the world.* Available at: http://www.creditcards.com/credit-card-news/ (accessed on: 13 June 2013).

Schwikkard, P.J. & Van der Merwe, S.E. 2005. *Principles of evidence.* (2nd edn.). Lansdowne: Juta Law.

Sewell, M. [Sa]. *The use of qualitative interviews in evaluation.* Available at: http://ag.arizona.edu(s)fcs/cyfernet/cyfar/Intervu5.htm (accessed on: 22 October 2013)

Shenton, A.K. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information,* 22:63-75. Available at: http://www.crec.co.uk/docs/Trustworthypaper.pdf (accessed on: 18 July 2013).

Smart Card Alliance. 2015. *EMV and NFC: Complementary technologies enabling secure contactless payments.* Available at: http://www.emv-connection.com (accessed on: 18 December 2015).

Smith, J.H. & Zinn, R.J. 2015. Developments in forensic technology (Pp. 397-433). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Snyman, C.R. 2006. *Strafreg. 5de uitgawe.* Durban: LexisNexus Butterworths.

South Africa. 1964. Customs and Excise Act, 1964 (Act No. 91 of 1964). Pretoria: Government Printer.

South Africa. 1977. Criminal Procedure Act, 1977 (Act No. 51 of 1977). Pretoria: Government Printer.

South Africa. 1995. South African Police Service Act, 1995 (Act No. 68 of 1995). Pretoria: Government Printer.

South Africa. 1996. Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996). Pretoria: Government Printer.

South Africa. 1998. Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998). Pretoria: Government Printer.

South Africa. 2001. Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001). Pretoria: Government Printer.

South Africa. 2002. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002). Pretoria: Government Printer.

South Africa. 2002. Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002). Pretoria: Government Printer.

South Africa. 2005. Government Notice No. R. 1263 of 29 December 2005. Government Gazette No. 28371. Pretoria: Government Printer.

South Africa. 2013. Criminal Law (Forensic Procedures) Amendment Act, 2013 (Act No. 37 of 2013). Pretoria: Government Printer.

South Africa. 2015. Cybercrimes and Cybersecurity Bill. Pretoria: Government Printer.

South African Banking Risk Information Centre. 2012. *Card Fraud South Africa 2011-2012.* Available at: https://www.sabric.co.za/Downloads/PDF-Documents(s)abric-Card-Fraud-Booklet-2011-2012.aspx (accessed on: 25 April 2013).

South African Banking Risk Information Centre. 2013a. *Different types of handheld card skimming devices.* Available at: https://www.sabric.co.za/Media-Centre/Image-Library/Different-Types-of-Handheld-Card-Skimming-Devices.aspx (accessed on: 10 August 2013).

South African Banking Risk Information Centre. 2013b. *Banking industry releases crime fraud statistics.* Available at: https://www.sabric.co.za/Media-Centre/Press-Releases/2013/2013-11/Banking-Industry-Releases-Crime-Fraud-Statistics.aspx (accessed on: 19 November 2013).

South African Banking Risk Information Centre. 2013c. *Card fraud South Africa 2013.* Available at: https://www.sabric.co.za/Downloads/PDF-Documents/Card-Fraud-SA-2013.aspx (accessed on: 11 March 2014).

South African Banking Risk Information Centre. 2013d. *Tactical Weekly Provincial Commercial Crime Risk Forecast 23/2013 for Gauteng for the period 23 June 2013 to 29 June 2013.*

South African Banking Risk Information Centre. 2014. *Card Fraud South Africa 2014.* Available at: https://www.sabric.co.za/media/1141/final-card-booklet.pdf (accessed on:15 July 2015).

South African Banking Risk Information Centre. 2015. *Card Fraud 2015.* Available at: https://www.sabric.co.za/media/1146/final-card-booklet.pdf (accessed on: 15 December 2015).

South African Police Service. 2003. *Conducting of docket inspections: Commercial Branch.* Head Office directive with reference 26/13/3. 16 May. Pretoria.

South African Police Service. 2005. *Commercial Crime: Implementation of an electronic mainframe photo album on Inkwazi: Banking crime suspects/accused.* Head Office directive with reference 3/21/3/1/51. 18 October.

South African Police Service. 2006a. *Commercial Crime: Implementation of banking crime spreadsheet: All reported banking crime cases.* Head Office directive with reference 3/21/3/1/51. 27 January.

South African Police Service. 2006b. *Joint Operational Forum Banking Crime: Weesgerus, Modimolle: 7 to 9 March 2006.* Head Office directive with reference 3/3/8/98/1. 13 February.

South African Police Service. 2006c. *Commercial crime: Sharing of information/intelligence and co-ordination of investigations.* Head Office directive with reference 3/21/3/1/51. 22 February.

South African Police Service. 2006d. *Conducting of docket inspections: Commercial Branch.* Head Office directive with reference 26/13/3. 14 August.

South African Police Service. 2006e. *Inkwazi: Co-ordination and research of commercial crime information and intelligence, photographs and other multimedia attachments. The inter-media research function and the spreadsheet upload function. Photographs of banking crime suspects and the banking crime spreadsheet.* Head Office directive with reference 3/21/3/1/98. 21 September.

South African Police Service. 2006f. *National Instruction 1 of 2006 Research in the Service.*

South African Police Service. 2006g. *Commercial Crime Forensic Learning Programme Level I.* Pretoria: Division Human Resource Development.

South African Police Service. 2007. *Commercial Crime: Banking crime spreadsheet. Links made between cases.* Head Office directive with reference 3/21/3/1/51. 30 November.

South African Police Service. 2009a. *Basic Crime Investigation Course.* Pretoria: Division Human Resource Development.

South African Police Service. 2009b. *Commercial Crime Forensic Learning Programme Level II.* Pretoria: Division Human Resource Development.

South African Police Service. 2009c. *Resolving of Crime Course (Detective Learning Programme).* Pretoria: Division Human Resource Development.

South African Police Service. 2009d. *National operational strategy and standing operating procedures to combat card skimming in South Africa.* Pretoria: Directorate for Priority Crime Investigation.

South African Police Service. 2010a. *Directorate for Priority Crime Investigation: Commercial Crime mandate.* Pretoria: Directorate for Priority Crime Investigation.

South African Police Service. 2010b. *Revised instructions for the analysis of skimming devices and other peripherals relating to the counterfeiting of debit and credit cards.* Head Office directive with reference 26/18/2. 19 August.

South African Police Service. 2010c. *Re: JOF Strategy: 23 November 2010 & Minutes of the JOF.* Email from Colonel B Grobler. 23 November.

South African Police Service. 2010d. *Implementation of the banking crime strategy which emanates from its October 2010 Joint Operation Forum held in Port Elizabeth.* Email from the Section Commander: Banking Crime, Directorate for Priority Crime Investigation. 23 December.

South African Police Service. 2011a. *Investigation, prevention and combating of crime. Working procedure: Automatic teller machine (ATM) fraud related matters*. Provincial Directive from the Provincial Commander: Commercial Crime, Western Cape. 28 February.

South African Police Service. 2011b. *Proposed national operational strategy and standing operating procedures to combat card skimming in South Africa.* 14 December.

South African Police Service. 2011c. *Commercial Crime Forensic Learning Programme Level III.* Pretoria: Division Human Resource Development.

South African Police Service. 2011d. *Standing Order (General) 324 Checking of case dockets.*

South African Police Service. 2011e. *National Instruction 3 of 2011 Registration of case dockets on the Crime Administration System (CAS).*

South African Police Service. 2011f. *Commercial Crime: Banking crime database. Links made with operational case data.* Head Office directive with reference 3/21/3/1/51. 10January.

South African Police Service. Annual Report 2011/12.

South African Police Service. 2012a. *Briefing of the newly appointed National Commissioner General Phiyega on 19 July 2012: DPCI Head Office, Promat Building, Silverton, Pretoria. Overview of Commercial Crime, DPCI.* Head Office information note with reference 3/1/1. 27 July.

South African Police Service. 2012b. *Resolving of Crime Course.* Pretoria: Division Human Resource Development.

South African Police Service. Annual Report 2012/13.

South African Police Service. Annual Report 2013/14.

South African Police Service. 2013a. *National Instruction 2 of 2013. The management of fingerprints, body-prints and photographic images.*

South African Police Service. 2013b. *Mandate of the Directorate for Priority Crime Investigation (DPCI): Influx of single case dockets (banking-related crime and advance fee fraud) to the DPCI.* Head Office directive with reference 3/7/1 over 3/9/4. 6 March.

South African Police Service. 2013c. *Standing operating procedures i.r.o. skimming devices to be followed by all Commercial Crime Units.* Head Office directive with reference 26/18/2. 6 December.

South African Police Service. 2013d. *Administration, Organisation and Control: Deployment of members on shifts in accordance to the Crime Threat and Crime Pattern Analysis.* Head Office directive with reference 3/1/5/1/203. 23 December.

South African Police Service. 2014. *Establishment of a steering committee for the South African Police Service and South African Banking Risk Identification Centre (Sabric). Partnership and nominations of teams to the Quick Win Plan.* Head Office directive with reference 3/5/2/293. 30 June.

South African Police Service. Annual Report 2014/15.

Stelfox, P. 2013. *Criminal investigation. An introduction to principles and practice.* New York, NY: Routledge.

Swanson, C.R., Chamelin, N.C. & Territo, L. 2003. *Criminal investigation*. (8th edn.). Boston: McGraw-Hill.

Taroni, F., Bozza, S., Biedermann, A., Garbolino, P. & Aitken, C. 2010. *Data analysis in forensic science. A Bayesian decision perspective.* West Sussex: John Wiley & Sons.

TestLink. 2014. *ATM glossary.* Available at: http://www.testlink.co.uk/glossary.html (accessed on: 24 June 2014).

United States Computer Emergency Readiness Team. 2008. *Computer forensics.* Available at: https://www.us-cert.gov(s)ites/default/files/publications/forensics.pdf (accessed on: 25 April 2013).

University of South Africa. 2012. *Policy on research ethics*. Available at: http://www.unisa.ac.za/contents/faculties(s)ervice_dept (accessed on: 12 April 2013).

Van der Westhuizen, J. (Ed.). 1996. *Forensic Criminalistics.* (2nd edn.). Durban: Heinemann.

Van Graan, J. & Budhram, T. 2015. Principles of investigation (Pp. 43-66). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Van Niekerk, T., Lochner, H., Naidoo, Y. & Zinn, R.J. 2015. The further investigation phase (Pp. 209-247). In R. Zinn and S. Dintwe. (Eds). *Forensic investigation. Legislative principles and investigative practice.* Cape Town: Juta.

Van Rooyen, H.J.N. 2008. *The practitioner's guide to forensic investigation in South Africa*. Pretoria: Henmar.

Verafin. 2011. *Reducing debit card fraud losses: Pinpointing compromised cards through the identification of common points of purchase.* Available at: http://info.verafin.com (accessed on: 14 June 2014).

Visa International. 2012. *System and method for identifying a point of compromise in a payment transaction processing system.* Available at: www.google.com/patents (accessed on: 11 June 2013).

Visa South Africa. 2012. *Growth in debit usage as South Africans look to manage their money more carefully.* Available at: https://www.visa.co.za (accessed on: 12 June 2013).

Visa USA. 2012. *Visa card security features.* Available at: http://usa.visa.com/download/merchants/card-security-features-mini-vcp-111512.pdf (accessed on: 23 May 2014).

3VR Incorporated. 2011. *Five best practices for using video surveillance to halt skimming fraud.* Available at: www.3vr.com (accessed on: 23 May 2013).

Welman, C., Kruger, F. & Mitchell, B. 2012. *Research methodology*. (3rd edn.). Cape Town: Oxford University Press.

Wendorff-Goerge, C. 2007. *New ATM security measures to tackle fraud. A*vailable at: http://www.atmmarketplace.com/articles/new-atm-security-measures-tackle-fraud/ (accessed on: 29 June 2014).

Zoldi, S., Wang, L., Sun, L. & Wu, S. 2007. *Mass compromise/ point of compromise analytic detection and compromised card portfolio management system.* Available at: http://www.sumobrain.com/patents/wipo/Mass-compromise-point-analytic-detection (accessed on: 15 March 2013).

CASE LAW

Lachman v The State (432/09) [2010] ZASCA 14

Ntsele v S [1998] 3 ALL SA 517 (A)

R v Heyne 1956 (3) SA 604 (A)

R v Larkins 1934 AD 91 94

Re London and Globe Finance Corporation Ltd 1903 1 Ch 728

S v Dube 2000 1 SACR 53 (N)

S v Mbokazi 1998 1 SACR 438 (N)

S v Myeza 1985 (4) SA 30 (T)

S v Nyembe 2014 (1) SACR 105 (GSJ)

S v Salcedo 2003 1 SACR 324 (SCA)

S v Van den Berg 1991 (1) SACR 104 (T)

LIST OF SAPS DOCKETS ANALYSED

No	SAPS Station	CAS no
1	Booysens	540/12/2012
2	Booysens	296/02/2013
3	Booysens	353/02/2013
4	Bramley	78/12/2012
5	Bramley	342/02/2013
6	Bramley	158/03/2013
7	Bramley	228/03/2013
8	Brixton	497/01/2013
9	Brixton	249/03/2013
10	Carletonville	19/12/2012
11	Carletonville	50/12/2012
12	Carletonville	73/12/2012
13	Carletonville	86/12/2012
14	Carletonville	87/12/2012
15	Carletonville	88/12/2012
16	Carletonville	282/12/2012
17	Carletonville	309/12/2012
18	Carletonville	313/12/2012
19	Carletonville	647/12/2012
20	Carletonville	518/02/2013
21	Carletonville	537/02/2013
22	Carletonville	188/03/2013
23	Carletonville	275/03/2013
24	Carletonville	536/03/2013
25	Douglasdale	926/11/2012
26	Douglasdale	172/12/2012
27	Douglasdale	285/12/2012
28	Douglasdale	496/12/2012

No	SAPS Station	CAS no
29	Douglasdale	761/12/2012
30	Douglasdale	531/01/2013
31	Douglasdale	612/01/2013
32	Douglasdale	803/01/2013
33	Douglasdale	180/02/2013
34	Hillbrow	299/12/2012
35	Hillbrow	300/12/2012
36	Hillbrow	449/12/2012
37	Hillbrow	450/12/2012
38	Hillbrow	456/12/2012
39	Hillbrow	659/12/2012
40	Hillbrow	662/12/2012
41	Hillbrow	913/01/2013
42	Hillbrow	212/02/2013
43	Hillbrow	525/02/2013
44	Hillbrow	325/03/2013
45	Jeppe	57/12/2012
46	Jeppe	703/12/2012
47	Jeppe	876/12/2012
48	Jeppe	211/01/2013
49	Johannesburg Central	194/12/2012
50	Johannesburg Central	252/12/2012
51	Johannesburg Central	256/12/2012
52	Johannesburg Central	520/12/2012
53	Johannesburg Central	1007/12/2012
54	Johannesburg Central	1033/12/2012
55	Johannesburg Central	219/01/2013
56	Johannesburg Central	274/01/2013
57	Johannesburg Central	674/01/2013

No	SAPS Station	CAS no
58	Johannesburg Central	1085/01/2013
59	Johannesburg Central	1359/01/2013
60	Johannesburg Central	1307/02/2013
61	Johannesburg Central	1096/03/2013
62	Linden	283/01/2013
63	Linden	670/01/2013
64	Linden	545/03/2013
65	Norwood	33/12/2012
66	Norwood	415/12/2012
67	Norwood	147/03/2013
68	Norwood	202/03/2013
69	Randburg	96/12/2012
70	Randburg	101/12/2012
71	Randburg	216/12/2012
72	Randburg	799/02/2013
73	Randburg	259/03/2013
74	Randburg	329/03/2013
75	Rosebank	163/01/2013
76	Rosebank	31/02/2013
77	Rosebank	163/02/2013
78	Rosebank	179/02/2013
79	Sandton	622/12/2012
80	Sandton	693/12/2012
81	Sandton	183/01/2013
82	Sandton	560/01/2013
83	Sandton	571/01/2013
84	Sandton	734/01/2013
85	Sandton	762/01/2013
86	Sandton	885/02/2013

No	SAPS Station	CAS no
87	Sandton	820/03/2013
88	Westonaria	50/12/2012
89	Westonaria	179/12/2012
90	Westonaria	272/12/2012
91	Westonaria	273/12/2012
92	Westonaria	48/01/2013
93	Westonaria	281/01/2013
94	Yeoville	199/12/2012
95	Yeoville	467/12/2012
96	Yeoville	26/01/2013
97	Yeoville	33/01/2013
98	Yeoville	59/02/2013
99	Yeoville	175/02/2013
100	Yeoville	275/02/2013

OTHER SAPS DOCKETS

No	SAPS Station	CAS no
1	Akasia	500/07/2013
2	Algoa Park	154/08/2010
3	Amersfoort	87/08/2012
4	Beaufort West	525/09/2013
5	Bedfordview	334/09/2013
6	Bethal	68/02/2013
7	Crystal Park	206/04/2013
8	Crystal Park	153/03/2013
9	Delmas	43/01/2012
10	Douglasdale	816/05/2013
11	Dunnotar	44/07/2013
12	Edenvale	27/09/2013
13	Garsfontein	527/08/2013
14	Hendrina	68/04/2012
15	Humewood	64/11/2014
16	Humewood	316/02/2012
17	Humewood	470/01/2012
18	ldutywa	11/08/2012
19	Kareedouw	49/08/2011
20	Kwazekele	569/08/2010
21	Kliptown	348/03/2014
22	Malamulele	144/08/2013
23	Malelane	20/09/2013
24	Middlelburg MP	309/10/2011
25	Milnerton	733/03/2013
26	Mount Road	387/04/2011
27	Nelspruit	206/11/2011
28	Norwood	383/07/2012

No	SAPS Station	CAS no
29	Park Road	880/10/2011
30	Parkview	84/10/2013
31	Potchefstroom	298/10/2013
32	Pretoria Central	1054/02/2014
33	Pretoria Central	847/11/2013
34	Pretoria Central	886/11/2013
35	Pretoria West	165/02/2014
36	Queenstown	29/11/2011
37	Sandton	441/04/2013
38	Sasolburg	185/08/2013
39	Seapoint	284/05/2013
40	Sunnyside	490/11/2013
41	Sinoville	487/04/2013
42	Uitenhage	426/01/2012
43	Villieria	43/05/2013
44	Volksrust	68/04/2013
45	Wierdabrug	205/03/2013
46	Wierdabrug	644/10/2013
47	Witbank	1045/10/2013
48	Winterton	21/09/2013

ANNEXURE A: PERMISSION TO CONDUCT RESEARCH WITHIN THE SAPS

G.P.-S. 002-0222 SAP 21

SUID-AFRIKAANSE POLISIEDIENS SOUTH AFRICAN POLICE SERVICE

Privaatsak/Private Bag X94

Reference Nr Verwysing	3/34/2
Navrae Enquiries	Col J Schnetler Lt Col GJ Joubert
Telefoon Telephone	012-393 3177 012-393 3118
Faksnommer Fax number	012-393 3178

STRATEGIC MANAGEMENT COMPONENT
HEAD OFFICE
PRETORIA

Lt-Col NDC Geldenhuys
COMMERCIAL CRIME

RE: RESEARCH REQUEST: IDENTIFICATION AS A TECHNIQUE TO INVESTIGATE COUNTERFEIT CARD FRAUD: NDC GELDENHUYS

1. Your research proposal pertaining to the above mentioned topic refers.
2. The study was approved by the Head: Directorate for Priority Crime Investigation (DPCI).
3. This office is in accord with the decision of the Head: DPCI. Approval is hereby granted in terms of National Instruction 1 of 2006.
4. You may therefore proceed with arrangements regarding the conducting of your study.

With kind regards,

_____ **MAJOR GENERAL**
HEAD: STRATEGIC MANAGEMENT
M MENZIWA

Date: 2013.03.12.

ANNEXURE B: INTERVIEW SCHEDULE: COUNTERFEIT CARD FRAUD INVESTIGATORS

Interview schedule **Participant No. .....**

(Counterfeit card fraud investigators)

An evaluation of identification methods used in the investigation of counterfeit card fraud

Section 1: Historical information

1. Are you a crime investigator?
2. If not, please state the field or environment in which you work.
3. For which company or organisation do you work?
4. For how many years (years of experience in the field)?
5. In which age group are you? (20-25 years; 26-30 years; 31-35 years; 36-40 years; 41-45 years; 46-50 years; 51-55 years; 56-60 years)
6. Please give a broad outline of your job functions.
7. In what type of crime investigation do you specialise (if any)?
8. Please specify your tertiary qualifications.
9. Give a summary of all formal and on-the-job training you have received in the field in which you are working.

Section 2: Forensic investigation in counterfeit card fraud cases

10. What is forensic investigation?
11. What is the purpose of forensic investigation?
12. What are the objectives of forensic investigation?
13. Have you investigated counterfeit card fraud cases?
14. What is the purpose of forensic investigation in counterfeit card fraud cases?
15. What is your understanding of fraud and the elements of fraud?
16. Have you investigated counterfeit card fraud resulting from the skimming of cards using the following methods?:
    (a) An automated teller machine (ATM) mounted skimming device
    (b) A handheld skimming device

(c) A point-of-sale (POS) device

17. Describe how counterfeit card fraud resulting from different methods/types of card skimming is committed.
18. What security feature(s) of bank cards is/are compromised when skimming of card data takes place?
19. Describe the different types of skimming devices, what they look like and how they work.
20. Describe what a PIN-capturing device is, what it looks like and how it works.
21. Have you been trained to investigate counterfeit card fraud? If so, elaborate.

Section 3: Identification in counterfeit card fraud cases

22. Are you familiar with the concept of 'identification' in forensic investigation?
23. If yes, explain the concept.
24. Are you familiar with the different types (categories) of identification in forensic investigation?
25. If yes, list them.
26. Do you use identification to investigate counterfeit card fraud?
27. If yes, how do you use identification to investigate counterfeit card fraud?
28. What is your understanding of the concept of 'individualisation'?
29. Do you use individualisation to investigate counterfeit card fraud cases?
30. If yes, how do you use individualisation to investigate counterfeit card fraud cases?
31. During the investigation of counterfeit card fraud cases resulting from card skimming, how would you identify and individualise the following?:
    (a) Fraudulent spend transactions (also known as negative spend or disputed transactions) on bank statements
    (b) The point of compromise or a common point of compromise (i.e. a common point of purchase) (CPP) of the original card(s) (the specific merchant, ATM or POS device and the location where the skimming and PIN capturing took place)
    (c) The skimming device and PIN-capturing device used
    (d) The person(s) who manufactured and/or supplied the skimming device and PIN-capturing device

(e) The person(s) who mounted the skimming device and PIN-capturing device onto the ATM, or used the handheld skimming device or POS device to skim the card(s)

(f) The person(s) who manufactured the counterfeit card(s)

(g) The equipment used to manufacture the counterfeit card(s)

(h) The merchant(s) and/or ATM(s) where the fraudulent spend took place using the counterfeit card(s) (i.e. point(s) of fraudulent/negative spend)

(i) The person(s) responsible for the fraudulent/negative spend

(j) The counterfeit card(s)

32. How would you, during investigation, identify and individualise the cardholder(s) whose card(s) had been compromised and counterfeited if a counterfeit card, skimming device, computer or other digital storage device (e.g. a memory stick, cellphone or compact disc) is seized/recovered and the cardholder(s) is/are unknown?

33. How can the South African Banking Risk Information Centre (Sabric) support or assist SAPS and bank investigators to do the following?:

(a) Identify and individualise points of card compromise

(b) Identify and individualise points of fraudulent spend

(c) Determine patterns, trends and tendencies in respect of counterfeit card fraud

34. How do you propose that SAPS and bank investigators approach single, unrelated counterfeit card fraud cases where the suspect, method of skimming, type of skimming device used and point of compromise are unknown, in order to improve the capabilities of investigators to effectively identify and individualise the following?:

(a) The points of card compromise

(b) The points of fraudulent spend takes place

(c) The person(s) responsible for the card skimming, PIN capturing and use of the counterfeit cards.

ANNEXURE C: INTERVIEW SCHEDULE: SOUTH AFRICAN BANKING RISK INFORMATION CENTRE

Interview schedule **Participant No. .....**

(South African Banking Risk Information Centre)

An evaluation of identification methods used in the investigation of counterfeit card fraud

Section 1: Historical information

1. Are you a crime investigator?
2. If not, please state the field or environment in which you work.
3. For which company or organisation do you work?
4. For how many years (years of experience in the field)?
5. In which age group are you? (20-25 years; 26-30 years; 31-35 years; 36-40 years; 41-45 years; 46-50 years; 51-55 years; 56-60 years)
6. Please give a broad outline of your job functions.
7. In what type of crime investigation do you specialise (if any).
8. Please specify your tertiary qualifications.
9. Give a summary of all formal and on-the-job training you have received in the field in which you are working.

Section 2: Forensic investigation in counterfeit card fraud cases

10. What is your understanding of fraud and the elements of fraud?
11. Describe how counterfeit card fraud resulting from different methods/types of card skimming is committed.
12. What security feature(s) of bank cards is/are compromised when skimming of card data takes place?
13. Describe the different types of skimming devices, what they look like and how they work.
14. Describe what a PIN-capturing device is, what it looks like and how it works (PIN refers to the personal identification number of the card holder).

Section 3: Identification in counterfeit card fraud cases

15. Explain the concept of ‘identification’.
16. Explain the concept of ‘individualisation’.
17. During the investigation of a counterfeit card fraud case resulting from card skimming, how do you propose that the investigator identify and individualise the following?:
    (a) Fraudulent spend transactions (also known as negative spend or disputed transactions) on bank statements
    (b) The point of compromise or a common point of compromise (i.e. a common point of purchase) (CPP) of the original card(s) (the specific merchant, ATM or POS device and the location where the skimming and PIN capturing took place)
    (c) The skimming device and PIN-capturing device used
    (d) The person(s) who manufactured and/or supplied the skimming device and PIN-capturing device
    (e) The person(s) who mounted the skimming device and PIN-capturing device onto the ATM, or used the handheld skimming device or POS device to skim the card(s)
    (f) The person(s) who manufactured the counterfeit card(s)
    (g) The equipment used to manufacture the counterfeit card(s)
    (h) The merchant(s) and/or ATM(s) where the fraudulent spend took place using the counterfeit card(s) (i.e. point(s) of fraudulent/negative spend)
    (i) The person(s) responsible for the fraudulent/negative spend
    (j) The counterfeit card(s)
18. How can the South African Banking Risk Information Centre (Sabric) support or assist SAPS and bank investigators to do the following?:
    (a) Identify and individualise points of card compromise
    (b) Identify and individualise points of fraudulent spend
    (c) Determine patterns, trends and tendencies in respect of counterfeit card fraud
19. How do you propose that SAPS and bank investigators approach single, unrelated counterfeit card fraud cases where the suspect, method of skimming, type of skimming device used and point of compromise are

unknown, in order to improve the capabilities of investigators to effectively identify and individualise the following?:

(a) The points of card compromise

(b) The points of fraudulent spend takes place

(c) The person(s) responsible for the card skimming, PIN capturing and use of the counterfeit cards.

ANNEXURE D: CARD SECURITY FEATURES: VISA AND MASTERCARD

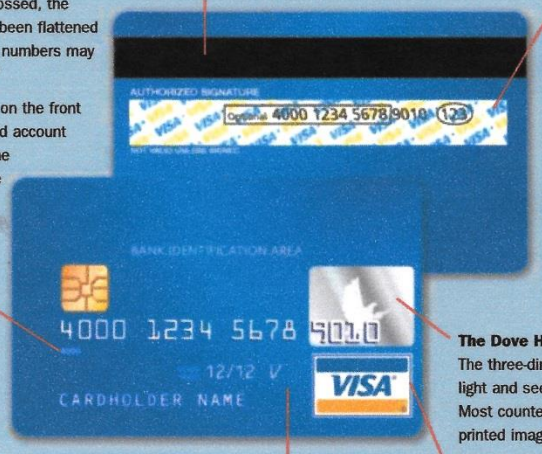
CARD IDENTIFICATION FEATURES

Security Features - Visa Flag Design with hologram

The Account Number
The account number must appear clear, clean and uniform. All Visa account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like "ghost images."

All or part of the account number on the front of the card must match the printed account number on the sales receipt. Some unembossed Visa cards may have only partial account numbers printed on the card.

Magnetic Stripe
The magnetic stripe should be smooth and straight, with no signs of tampering.



Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

Security Character
Visa cards may have a stylized "V" security character embossed to the right of the expiration date.

The Signature Panel
Make sure that the repetitive Visa name, printed in blue and gold at 45-degree angle, is clearly visible on the signature panel.

The card account number, plus a 3 digit Card Verification Value 2 (CVV2) is reverse indent-printed on the signature panel. Some cards will have only the last 4 digits of the account number plus the 3 digit CVV2, on the signature panel.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word "void" appears if the panel has been erased or compromised.

The Dove Hologram
The three-dimensional dove hologram should reflect light and seem to change as you rotate the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.

Visa Brand Mark
The Visa Brand Mark must appear in either the bottom or upper right corner. There is a microtext border.

All cards featuring this design will be discontinued by 30 June 2011.

Security Features — Mini Hologram on Card Back

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word "VISA" is repeated and visible on the panel when placed under an ultraviolet light.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word "void" appears if the panel has been erased or compromised. The manufacturer's ID is printed underneath the signature panel.

The Mini Dove Hologram
When the Mini Dove Design Hologram is used, it must appear on the back of the card. For non-Chip cards, it may be placed either below or to the left or right of the signature panel. For Chip cards, it is placed below the signature panel.

Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

Magnetic Stripe
The magnetic stripe should be smooth and straight, with no signs of tampering.

CVV2
The three-digit code (CVV2) may appear in the white box to the right of the signature panel or be reverse ident-printed onto the signature panel.

The Account Number
The 16-digit account number must appear clear, clean and uniform in size and spacing. All Visa account numbers begin with 4.

Visa Brand Mark
The Visa Brand Mark must appear in either the bottom right, top left or top right corner. Most cards will be horizontal in orientation. Visa cards with a chip may have a vertical orientation.

A "V" is visible over the Visa Brand Mark when placed under an ultraviolet light.

(Source: http://www.visa.ca/merchant/resources, accessed on: 26 January 2016)

CARD IDENTIFICATION FEATURES

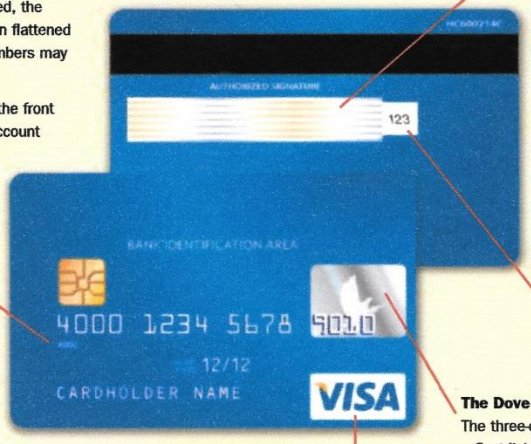
Security Features — Hologram on Card Front

The Account Number
The account number must appear clear, clean and uniform. All Visa account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like "ghost images."

All or part of the account number on the front of the card must match the printed account number on the sales receipt. Some unembossed Visa cards may have only partial account numbers printed on the card.

Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

Magnetic Stripe
The magnetic stripe should be smooth and straight, with no signs of tampering.



Visa Brand Mark
The Visa Brand Mark must appear in either the bottom right, top left or top right corner. A "V" is visible over the Visa Brand Mark when placed under an ultraviolet light.

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word "VISA" is repeated and visible on the panel when placed under an ultraviolet light.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word "void" appears if the panel has been erased or compromised.

CVV2
The three-digit code (CVV2) may appear in the white box to the right of the signature panel or be reverse ident printed onto the signature panel.

The Dove Hologram
The three-dimensional dove hologram should reflect light and seem to change as you rotate the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.

Security Features — HoloMag on Card Back

1 Microtext with the word "Visa" repeated.
2 When the card is tipped the dove appears to travel on top of the vertical lines.
3 Move the card side to side and the black dot will appear and disappear behind the dove.
4 Move the card up and down and the word "Visa" appears in the sun.

Holographic Magnetic Stripe
When the holomag is present on the card it must always be on the card back, and no other hologram appears on the card.

The Account Number
The account number must appear clear, clean and uniform. All Visa account numbers begin with 4. If a card has been re-embossed, the original embossed numbers have been flattened and new numbers embossed, the numbers may appear fuzzy, like "ghost images."

Bank Identification Number
The first four numbers of the account number must appear below the account number. These four numbers are the Bank Identification Number (BIN). If the two numbers do not match, the card has been altered or is counterfeit.

The Signature Panel
The signature panel must appear on the back of the card. It may look like this or be custom designed. The word "VISA" is repeated and visible on the panel when placed under an ultraviolet light.

Check for signs of tampering such as scratching, white tape or white correction fluid applied over the panel, or writing over another name with a felt-tip pen. The repeated word "void" appears if the panel has been erased or compromised.

CVV2
The three-digit code (CVV2) may appear in the white box to the right of the signature panel or be reverse ident printed onto the signature panel.

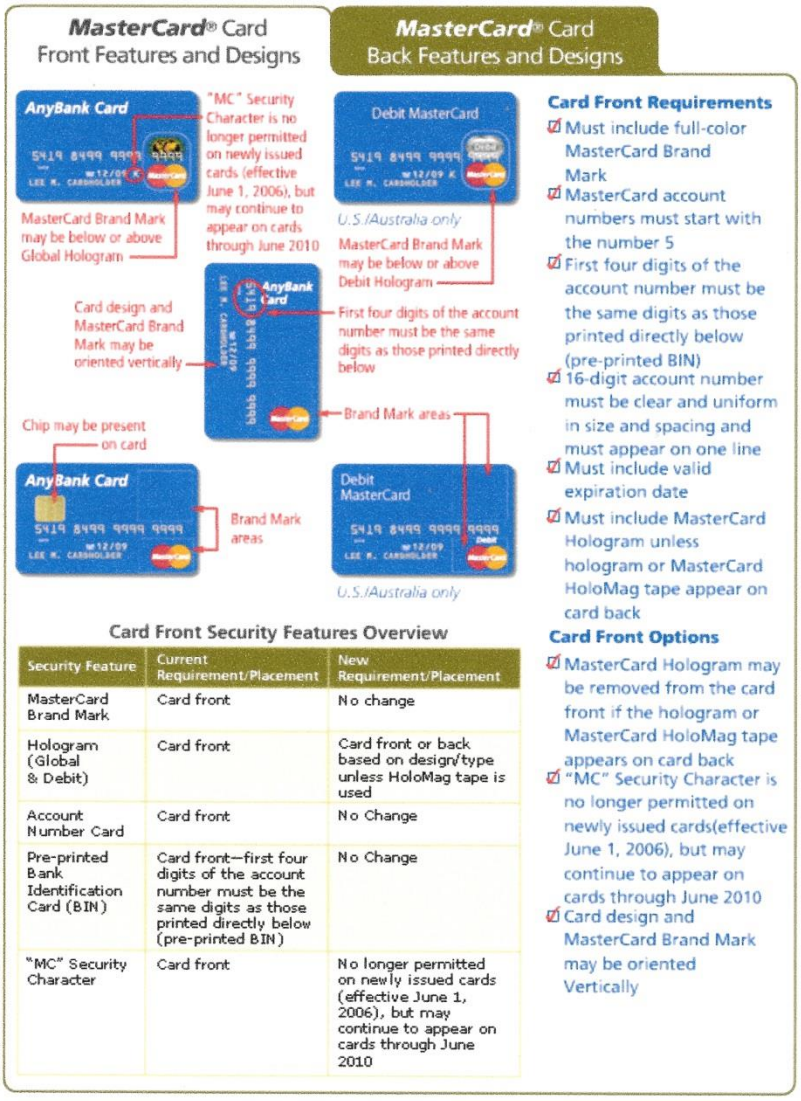
Visa Brand Mark
The Visa Brand Mark must appear in either the bottom right, top left or top right corner. A "V" is visible over the Visa Brand Mark when placed under an ultraviolet light.

MasterCard Card Identification Features

New Card Design Options and ID Features

MasterCard has introduced new card design format options and modified several card security features. New card design options offer flexible placement of the MasterCard hologram (card front or back) and introduce the option to use a new holographic magnetic tape, HoloMag™ (card back only). This reference page highlights valid card formats, as well as mandated card security features.

In the event that you are suspicious about a MasterCard card, call your Voice Authorisation Centre and request a Code 10.



Card Front Security Features Overview

Security Feature	Current Requirement/Placement	New Requirement/Placement
MasterCard Brand Mark	Card front	No change
Hologram (Global & Debit)	Card front	Card front or back based on design/type unless HoloMag tape is used
Account Number Card	Card front	No Change
Pre-printed Bank Identification Card (BIN)	Card front—first four digits of the account number must be the same digits as those printed directly below (pre-printed BIN)	No Change
"MC" Security Character	Card front	No longer permitted on newly issued cards (effective June 1, 2006), but may continue to appear on cards through June 2010

(Source: http://www.mastercard.com, accessed on: 26 January 2016)

MasterCard Card Identification Features

New Card Design Options and ID Features

MasterCard has introduced new card design format options and modified several card security features. New card design options offer flexible placement of the MasterCard hologram (card front or back) and introduce the option to use a new holographic magnetic tape, HoloMag™ (card back only). This reference page highlights valid card formats, as well as mandated card security features.

In the event that you are suspicious about a MasterCard card, call your Voice Authorisation Centre and request a Code 10.

MasterCard® Card Front Features and Designs | **MasterCard® Card Back Features and Designs**

Card Back Requirements

- ☑ Must include signature panel with the word "MasterCard" printed in multicolors at a 45° angle
- ☑ Last four digits of the account number must be printed in reverse italics on the signature panel
- ☑ CVC 2 number (three-digit validation code) must be printed in reverse italics to the right of the last four digits of the account number
- ☑ Magnetic tape must be present and appear smooth and straight with no signs of tampering
- ☑ Must include MasterCard Hologram or HoloMag tape unless hologram appears on card front

Card Back Options

- ☑ HoloMag tape may be used in place of the traditional magnetic tape
- ☑ MasterCard Hologram may be placed on the card back if not appearing on card front

Card Back Security Features Overview

Security Feature	Current Requirement/Placement	New Requirement/Placement
Hologram (Global & Debit)	Card front	Card front or back based on design/type unless HoloMag tape is used
HoloMag Tape	N/A—new security feature	Card back unless MasterCard Hologram is used
Last Four Digits of Account Number	Card back—printed in reverse italics in the upper center of the signature panel	Card back—printed in reverse italics in the upper right corner of the signature panel (permitted now, required after June 1, 2006)
CVC 2 Number	Card back—printed in reverse italics in the upper center of the signature panel to the right of the last four digits of the account number	Card back—printed in reverse italics in an adjacent white box to the right of the signature panel (permitted now, required after June 1, 2006)

ANNEXURE E: IMAGES OF CARDS, CARD SKIMMING, PIN-CAPTURING AND CARD COUNTERFEITING DEVICES AND EQUIPMENT

Figure 1: A magnetic stripe card and white plastic cards used to manufacture counterfeit cards

(Source: www.made-in-china.com, accessed on: 2 November 2013)

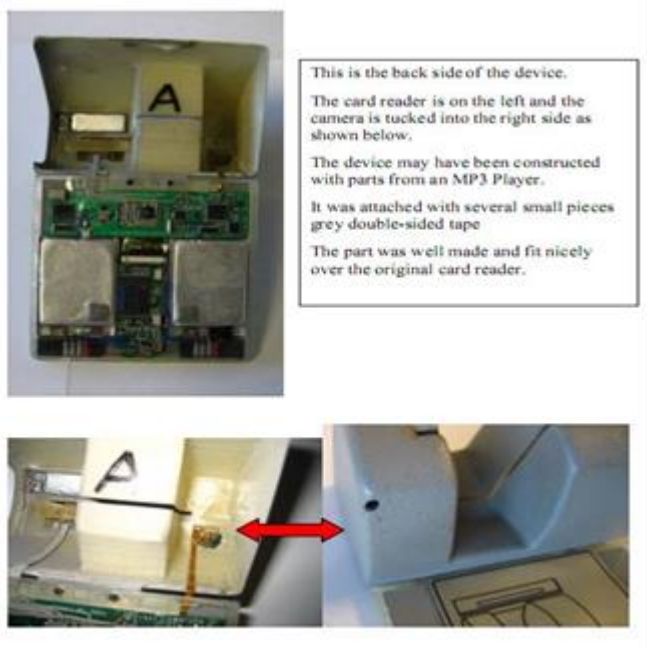
Figure 2: Chip-and-pin cards (also called smart cards, integrated circuit (IC) cards)

(Sources: www.standardbank.co.za and www.pcmag.com, accessed on: 2 November 2013)

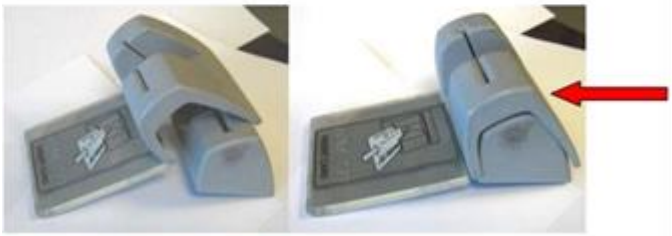
Figure 3: Handheld skimming devices

(Sources: www.made-in-china.com; www.sabric.co.za, accessed on: 2 November 2013; SABRIC, 2014a:21; 2015:22)

Figure 4: ATM skimming device (false card slot overlay)



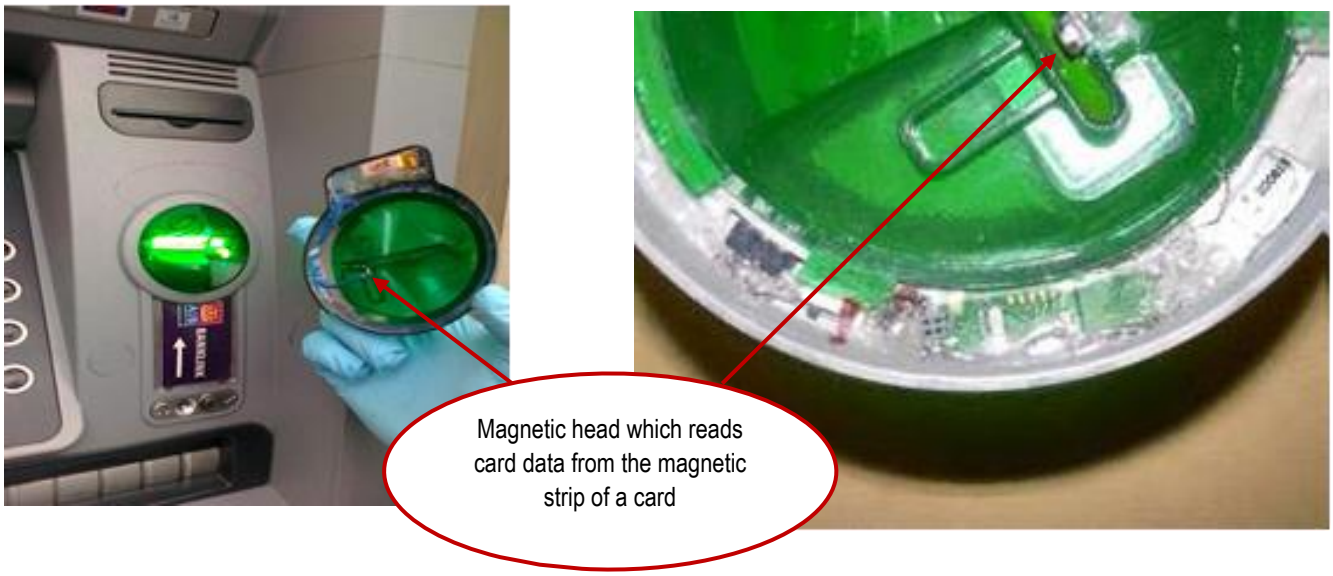
The real card reader slot. The capture device

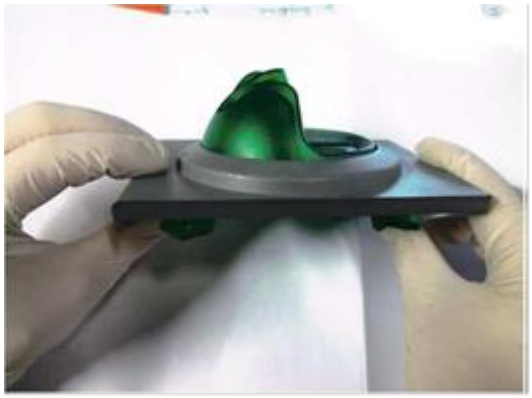


The side cut out is not visible when on the ATM.

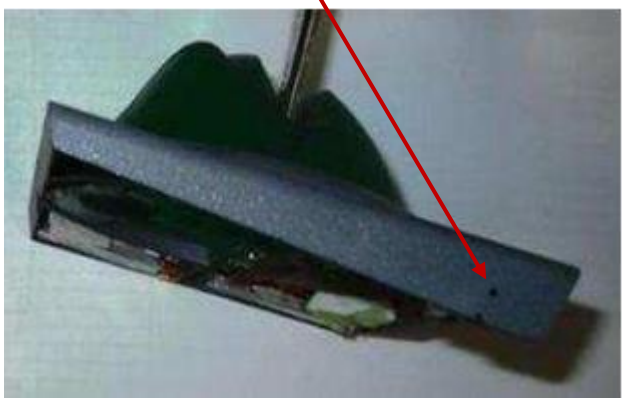
(Source: www.krebsonsecurity.com, accessed on: 2 November 2013)

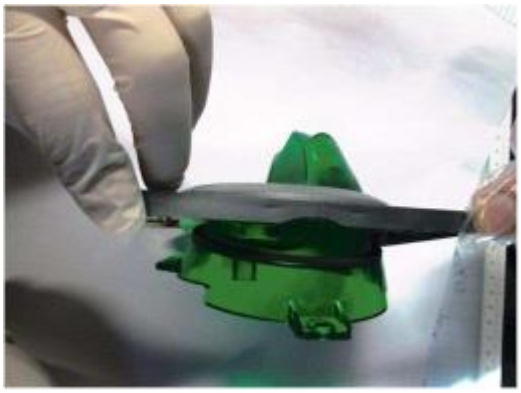
Figure 5: ATM skimming devices and PIN-capturing devices

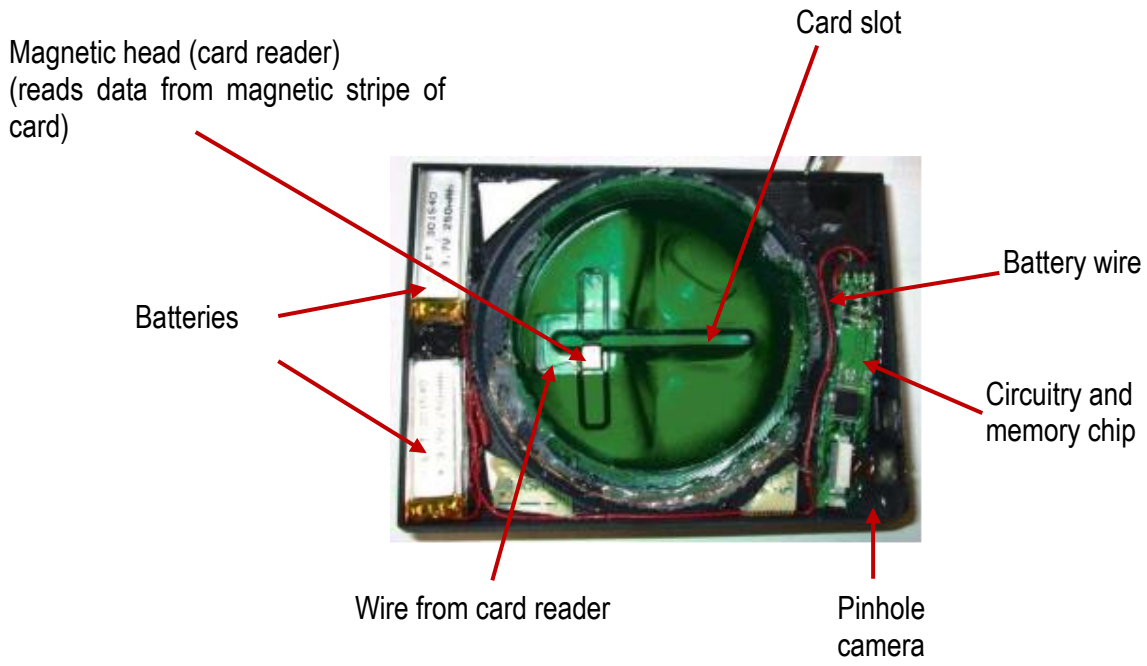




Pinhole for micro-camera in false fascia segment







(Sources: www.krebsonsecurity.com, accessed on: 2 November 2013; European ATM Security Team, emails dated 2014/02/04 and 2014/04/04; Norwood CAS 383/07/2012; SABRIC, 2014a:23)

Figure 6: PIN-capturing devices used on ATMs

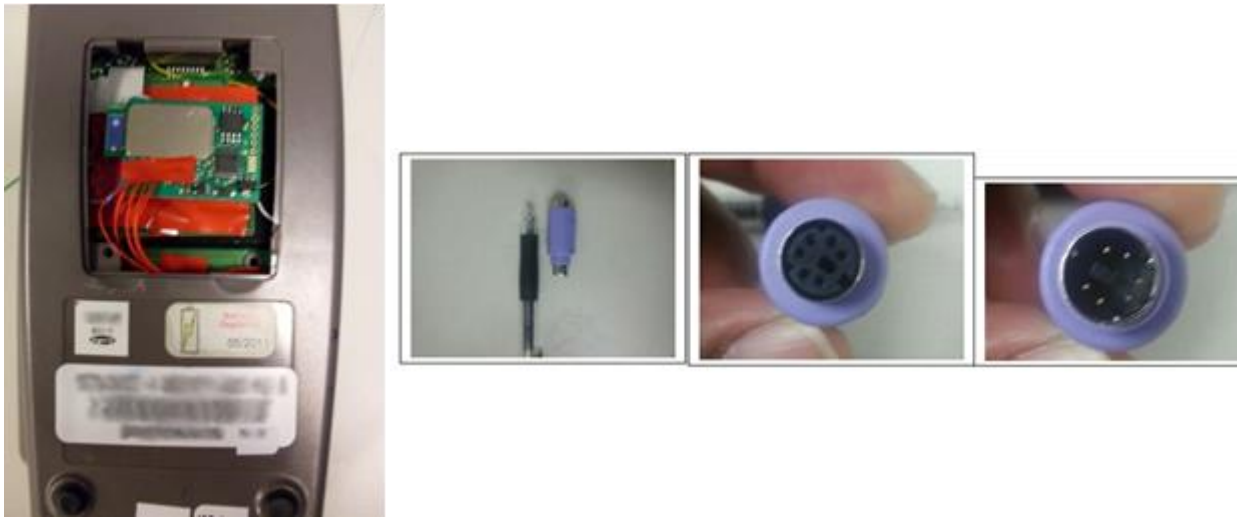
(Sources: www.spytechs.com; www.krebsonsecurity.com, accessed on: 2 November 2013)

(Source: Norwood CAS 383/07/2012)

Figure 7: Interface of a point-of-sale device, as advertised online, that can be used for card skimming

(Source: http:/(s)zlikes.en.made-in-china.com, accessed on: 2 November 2013)

Figure 8: The bottom of a point-of-sale device which was adapted to skim and record card data and PIN numbers (photo on the left), and cash register skimmers

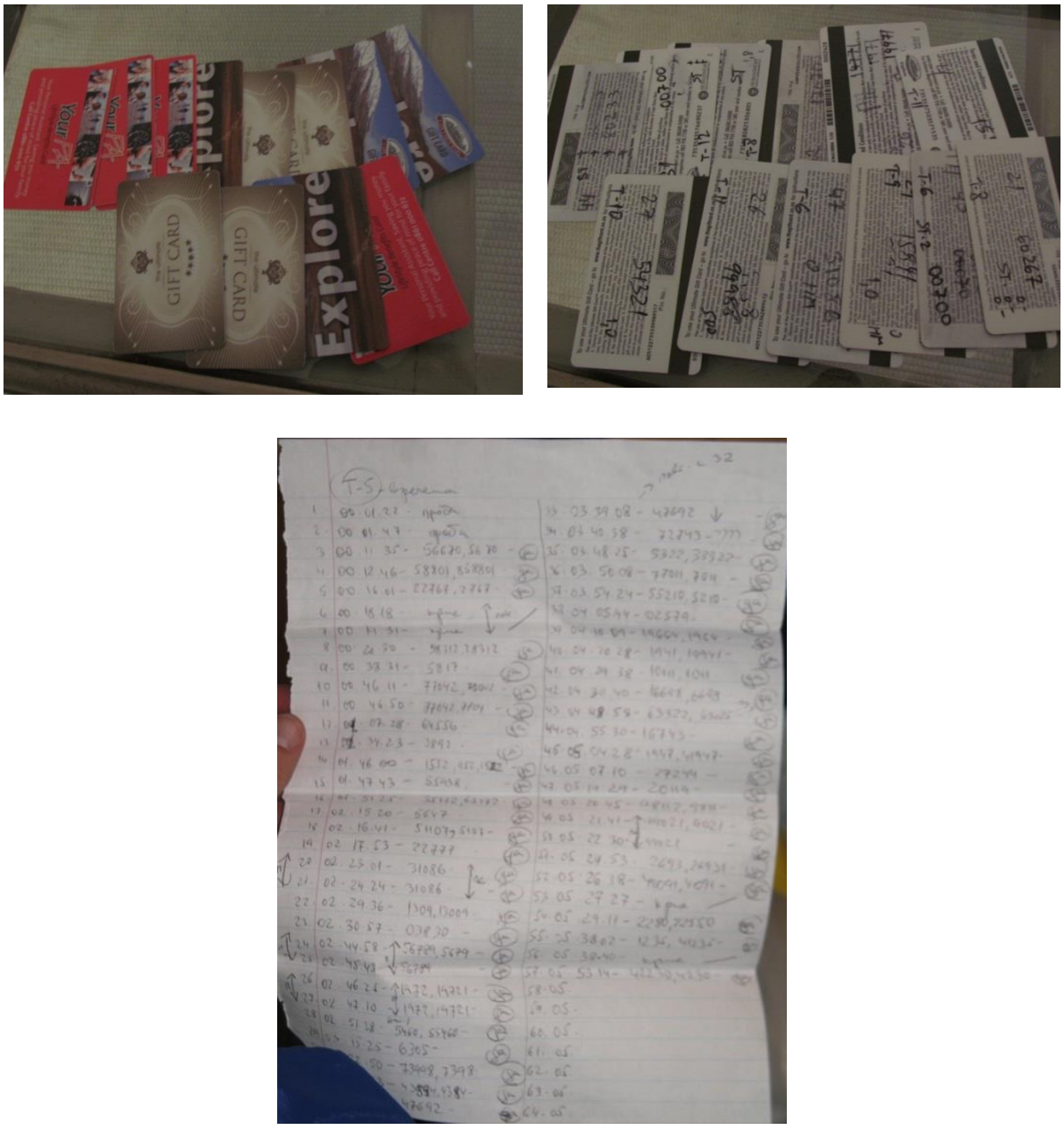


(Source: www.krebsonsecurity.com, accessed on: 2 November 2013)

Figure 9: Card reader/writer (encoder) combinations for sale on the Internet

(Sources: www.made-in-china.com and www.magstripe.com, accessed on: 2 November 2013)

Figure 10: Counterfeit cards with handwritten notes of PIN numbers



(Source: Norwood CAS 383/07/2012)

ANNEXURE F: SUMMARY OF SAPS COUNTERFEIT CARD FRAUD DOCKETS IN RESPECT OF WHICH OFFICIAL REPORTS WERE PERUSED, WHERE SUSPECTS HAVE BEEN IDENTIFIED POSITIVELY AND THE CRIME HAS BEEN INDIVIDUALISED

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
1	Eastern Cape 26/18/2 dated 8 April 2014	Butterworth	233/01/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*	*		*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device and counterfeit card(s).	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device and counterfeit card(s).	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
2	Eastern Cape 26/18/2 dated 8 April 2014	Butterworth	178/06/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*	*		*Direct arrest made by complainant (victim of card skimming) who is a police official. **Digital forensic examination of skimming device and counterfeit card(s).	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device and counterfeit card(s).	*Y **Y	*Y **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
3	Eastern Cape 26/18/2 dated 8 April 2014	Cofimvaba	32/08/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Alert bank official(s) identified suspect as a known card skimmer and counterfeit card fraudster and informed police. Other SAPS official(s) followed up the information. **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
4	Eastern Cape 26/18/2 dated 8 April 2014	Cofimvaba	131/10/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information re card skimming received from member of public and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from	*Y **Y	*N **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
											skimming device.								
5	Eastern Cape Email dated 15 October 2012	Humewood	454/06/2011	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users).	**	**		**		**Surveillance camera footage at ATMs. **Digital forensic examination of counterfeit cards.	**Arrests, search and seizure. **Victims identified by means of encoded, skimmed card data (account numbers) found on counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
6	Eastern Cape Email dated 15 October 2012	Humewood Humewood	316/02/2012 170/02/2012	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users).	**	**				**Physical undercover surveillance of ATM. **Surveillance camera footage.	**Arrest and search. **Suspect positively identified.	**Y	**Y	**Y	**Y	**N	**N	**Y	**Y
7	Eastern Cape 26/18/2 dated 8 April 2014	Idutywa	11/08/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).	**	*				**Camera surveillance footage of card skimming activities at ATM.	**Suspects linked to an existing case previously reported (in which they have been charged) and positively identified by means of camera surveillance footage.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
8	Eastern Cape Email dated 15 October 2012	Kareedouw	49/08/2011	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users).	**	**				**Surveillance camera footage at ATMs. **Analysis of ATM electronic transaction journals.	**Arrests. **Victims identified by means of ATM transaction journals where camera footage of skimming activities and fraudulent withdrawals corresponded with transaction time stamps done at ATMs.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
9	Eastern Cape Email dated 15 October 2012	Kwazakele East London Kwadwesi Adelaide Kwanobuhle	569/08/2010 925/08/2010 138/11/2010 41/12/2010 205/09/2010 13/02/2011 631/11/2010	ATM skimming. ATM mounted skimming devices. ATMs in different areas in Eastern Cape.	**	**		**		**Surveillance camera footage gathered at ATMs by security firm appointed by the bank. **Digital forensic examination of counterfeit cards. **Analysis of electronic ATM	**Suspects positively identified from surveillance camera footage and linked with fraudulent withdrawals from ATMs. **Arrests, search and	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized: Skimming device(s)	Exhibits seized: Counterfeit card(s)	Exhibits seized: Other relevant equipment	Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
		Kwazakhele Walmer								journals.	seizure of counterfeit cards. **Victims identified by means of encoded skimmed card data (account numbers) found on counterfeit cards. **Additional victims identified whose cards have been compromised using ATM transaction journals.								
10	Eastern Cape 26/18/2 dated 8 April 2014	Maclear	80/09/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information (complaint) re card skimming received from victim and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Additional victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*Y **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
11	Eastern Cape 26/18/2 dated 8 April 2014	Matatiele	43/03/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Suspects offering unsolicited help to customers and skimming cards identified at ATM through real-time camera surveillance of ATM by security firm appointed by bank. **Digital forensic examination of skimming device.	*Arrest(s) made by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*Y **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
12	Eastern Cape 26/18/2 dated 8 April 2014	Matatiele	108/03/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victim identified by means of skimmed card data (account number) downloaded from	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
											skimming device.								
13	Eastern Cape Email dated 15 October 2012	Mount Road	387/04/2011	ATM skimming. ATM mounted skimming device. ATM close to a shop in Port Elizabeth.	**	**	**	**	**	**Physical identification of skimming device and PIN-capturing device (pinhole camera). **Physical surveillance of ATM. **Suspects' addresses identified from GPS found in vehicle. **Search of vehicle and residential address. **Digital forensic examination of skimming device, counterfeit cards, computer harddrives, memory cards and memory chips.	**Arrests, search and seizure of skimming device, micro camera and a large amount of skimming related equipment and tools. **Victims identified by means of skimmed card data (account numbers) found during digital forensic examination of skimming device, counterfeit cards and digital storage devices (skimmed card data of 1 490 cards found).	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
14	Eastern Cape 26/18/2 dated 8 April 2014	Mqanduli	38/07/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information (complaints) re card skimming from card holders who were targeted received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure made by other SAPS official(s). **Additional victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*Y **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
15	Eastern Cape 26/18/2 dated 8 April 2014	Mqanduli	95/01/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*	*		*Information re card skimming received and followed up by other SAPS official(s). **Digital forensic examination of skimming device and counterfeit cards.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device and counterfeit cards.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
16	Eastern Cape 26/18/2 dated 8 April 2014	Mthatha	591/10/2011	Handheld skimming. Handheld skimming device. POC unknown.	*	**	**	**	**	**Information re card skimming/ counterfeit card fraud received and followed up by investigating officer.	**Arrest(s), search and seizure by investigating officer. **Victims identified by	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										**Digital forensic examination of skimming device, counterfeit card(s) and cell phone of suspect.	means of skimmed card data (account numbers) downloaded from skimming device and counterfeit card(s). **Additional suspect identified through digital forensic examination of cell phone.								
17	Eastern Cape 26/18/2 dated 8 April 2014	Mthatha	574/04/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
18	Eastern Cape 26/18/2 dated 8 April 2014	Mthatha	963/12/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Suspects targeting ATM customers identified by security guard at ATM, made the arrests and handed suspects over to other SAPS official(s). **Digital forensic examination of skimming device.	**Additional victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
19	Eastern Cape 26/18/2 dated 8 April 2014	Mthatha	181/09/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*	*		*Information re card skimming received and followed up by other SAPS official(s). **Digital forensic examination of skimming device and counterfeit cards.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device and counterfeit cards.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
20	Eastern Cape 26/18/2 dated 8 April 2014	Ngangelizwe	85/02/2012	Handheld skimming. Handheld skimming device. POC unknown.		*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										of skimming device.	skimmed card data (account numbers) downloaded from skimming device.								
21	Eastern Cape 26/18/2 dated 8 April 2014	Ngangelizwe	49/05/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*	*	*	*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device and counterfeit cards.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device and counterfeit cards.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
22	Eastern Cape 26/18/2 dated 8 April 2014	Qumbu	149/12/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*		*	*Information (complaint) re card skimming received from victim by security officer at ATM who arrested and handed suspect over to other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Additional victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*Y **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
23	Eastern Cape 26/18/2 dated 8 April 2014	Tsolo	200/10/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Information re card skimming received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
24	Eastern Cape Email dated 15 October 2012	Uitenhage Queenstown Algoa Park	426/01/2012 29/11/2011 154/08/2010	Unknown	**	**				**Point of fraudulent spend (ATM where fraudulent withdrawals were made) identified by means of collective analysis of negative spend on compromised accounts). **Surveillance cameras placed by SAPS at identified point.	**Arrest and search. **Victims identified by means of ATM transaction journal (date and time stamp of fraudulent transactions linked to known suspect identified from camera surveillance footage).	**Y	**Y	**Y	**Y	**N	**N	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										**Suspect known to SAPS investigators and identified from surveillance footage. **ATM transaction journal used to identify fraudulent transactions.									
25	Free State Email dated 15 October 2012	Park Road	99/10/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).		*	*			*Suspect arrested by other SAPS official(s) following card skimming activities at ATM. **Search of suspect's home. **Digital forensic examination of skimming device and suspect's cell phone.	*Arrest, search of suspect and seizure of skimming device by other SAPS official(s). **Search of home yielded no result. **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device. **Examination of cell phone did not yield positive results.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
26	Free State Email dated 15 October 2012	Park Road	880/10/2011	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).	**	**	**			**Common point of compromise (i.e. common point of purchase) (CPP) (ATM) positively identified by means of a collective analysis of positive spend transaction history of different compromised accounts. **Suspect arrested skimming cards at identified CPP. **Search of suspect's home. **Digital forensic examination of skimming device and suspect's cell phone.	**A specific ATM positively identified as a CPP. **Arrest, search of suspect and seizure of skimming device. **Search of home did not yield positive results. **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device. **Cell phone analysis did not yield positive results.	**Y	**Y	**y	**Y	**Y	**Y	**Y	**Y
27	Free State Email dated 14 May 2014	Sasolburg	185/08/2013	Handheld skimming. Handheld skimming device. At ATM.	*	*	*	*		*Real-time camera surveillance by bank's security company. **Digital forensic examination	*Arrest, search and seizure. **Victims identified by means of card data	*Y **Y	*Y **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										of skimming device and counterfeit cards.	(account numbers) retrieved from skimming device and counterfeit cards.								
28	Free State Email dated 15 October 2012	Sasolburg	178/06/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).	**	**	**			**Surveillance of ATM. **Digital forensic examination of skimming device.	**Arrest, search of suspect(s) and seizure of skimming device. **Victim(s) identified by means of skimmed card data (account number(s)) downloaded from skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
29	Free State Email dated 14 May 2014	Thabong	171/08/2013	Handheld skimming. Handheld skimming device. POC unknown.	**	**	**	**	**	**Information received of suspects and their address followed up. **Digital forensic examination of skimming device, laptop, card writer, memory stick and cell phone.	**Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device, laptop and card writer.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
30	Free State Email dated 15 October 2012	Virginia	60/09/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).	*	*	*			*Suspect arrested by other SAPS official(s) following card skimming activities at ATM. **Digital forensic examination of skimming device.	*Arrest, search of suspect and seizure of skimming device by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
31	Free State Email dated 14 May 2014	Zamdela	261/04/2013	Handheld skimming. Handheld skimming device. At ATM located inside shop.	*	*	*			*Information of suspect skimming cards received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
32	Gauteng Email dated 13 May 2014	Bedfordview	29/09/2013	Handheld skimming. Handheld skimming device.	**	**	**		**	**Physical undercover surveillance of ATMs. **Digital forensic examination	**Arrest, search and seizure. **Victims identified	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
				At ATMs (targeting ATM users) in Eastgate Mall.						of skimming device.	whose cards had been compromised by means of card data (account numbers) retrieved from skimming device during digital forensic examination.								
33	Gauteng Email dated 13 May 2014	Dunnottar	44/07/2013	Unknown (no skimming device was seized)	**	**		**	**	**Positive identification of suspects by name (as per information received. **Interrogation of suspects. **Search of suspect and addresses. **Digital forensic examination of counterfeit cards.	**Arrest, search and seizure. **Victims identified by means of skimmed encoded card data (account numbers) retrieved from counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
34	Gauteng Email dated 13 May 2014	Kempton Park	869/05/2013	Handheld skimming. Handheld skimming device. At ATM (targeting ATM users.	*	*	*			*Physical surveillance of ATM by bank's security company. **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of digital forensic examination of skimming device.	*Y **Y	*N **Y	*Y **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
35	Gauteng Email dated 13 May 2014	Moffatview	297/05/2013	Handheld skimming. Handheld skimming device. Petrol station (pump attendants).	**	**	**	**		**Search of suspects. **Interrogation of suspects.	**Arrest, search and seizure. **A third suspect (who supplied skimming device) identified and arrested from information obtained during interrogation of first two suspects.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
36	Gauteng Report dated 27 July 2012	Norwood	383/07/2012	ATM skimming. ATM mounted skimming device. ATM at a petrol station in Norwood.	**	**	**	**	**	**Information re card skimming/ counterfeit card fraud received and followed up. **Search of suspect's vehicle and house.	**Arrest(s), search and seizure. **Computers and other equipment seized in suspect's vehicle and house.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										**Digital forensic examination of skimming device, counterfeit cards, computers and cell phones .	**Victims identified by means of skimmed card data (account number(s)) downloaded from skimming devices and counterfeit cards.								
37	Gauteng Email dated 13 May 2014	Pretoria West	591/05/2013	Handheld skimming. Handheld skimming devices. POC unknown.	**	**	**	**	**	**Vehicle matching description and registration number traced with suspect. **Interrogation of suspect. **Digital forensic examination of skimming devices, counterfeit cards, laptops and cell phones.	**Arrest, search and seizure. **A further suspect arrested based on information obtained through interrogation. **Victims identified by means of skimmed card data (account numbers) obtained during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
38	Gauteng Email dated 13 May 2014	Randburg	466/04/2013	ATM skimming. ATM mounted skimming devices. ATMs in Gauteng.	**	**	**	**		**Physical surveillance of relevant ATM. **Searching of vehicles and residential addresses of suspects. **Digital forensic examination of skimming devices, counterfeit cards and cell phone.	**Arrest, search and seizure. **Victims identified by means of skimmed card data (account numbers) found on skimming devices and counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
39	Gauteng Email dated 13 May 2014	Randburg	407/06/2013	Handheld skimming. Handheld skimming device. At petrol station (petrol attendant).	**	**	**			**Interrogation of suspect. **Search of suspect. **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of skimmed card data downloaded during digital forensic examination of skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
40	Gauteng Email dated 13 May 2014	Sandton	441/04/2013	ATM skimming. ATM mounted skimming devices. ATMs in Gauteng.	**	**	**	**	**	**Sharing of intelligence and deploying a joint investigation team consisting of bank investigators, security companies and SAPS	**ATM mounted skimming device on ATM identified. **Suspect mounting skimming device to ATM	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										Commercial Crime Unit. **Surveillance camera footage at ATM. **Physical surveillance of relevant ATM (point of compromise). **Searching of vehicles and residential addresses of suspects. **Interrogation of suspects and extracting information. **Fingerprint examination of skimming devices, counterfeit cards and related equipment. **DNA examination of skimming devices, counterfeit cards and related equipment. **Digital forensic examination of skimming devices, counterfeit cards, digital storage devices and cell phones. **Modus operandi (construction method of ATM skimming devices and materials used).	identified from camera surveillance footage. **Suspect removing skimming device identified during physical surveillance of ATM, arrested and skimming device seized. **Further suspects arrested, skimming devices, counterfeit cards and related equipment seized as a result of searching vehicles and residences, and information obtained during interrogation. **Suspects linked to skimming devices and counterfeit cards by means of fingerprints. **Skimmed card data of 2 364 compromised cards obtained by means of digital foernsic analysis of skimming devices, and victims identified with account numbers. **Case linked to cases in Durban on the basis of similar construction method of skimming devices (modus operandi).								
41	Gauteng Email dated 13 May 2014	Sharpeville	993/06/2013	Handheld skimming. Handheld skimming devices. ATMs in Sharpeville,	**	**	**	**	**	**Collective/joint analysis of positive spend transaction data of different compromised accounts.	**Specific ATM positively identified as a common point of compromise.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
				Vereeniging, Sasolburg, Dube) (targeting ATM users).						**Recorded surveillance camera footage of suspects skimming cards. **Photographs of suspects. **Sharing of intelligence between role players of a joint investigation team comprising bank investigators, security firmas and police investigators. **Physical surveillance of ATM (POC). **Real-time camera surveillance of ATM (POC). **Interrogation of arrested suspect and follow-up of extracted information. **Search of residential address of suspect and seizure of exhibits. **Digital forensic examination of skimming devices, counterfeit cards and cell phones.	**Suspects responsible for card skimming identified. **Arrest, search and seziure. **Victims identified by means of skimmed card data downloaded during digital forensic examination of skimming devices, counterfeit cards and cell phones.								
42	Gauteng Email dated 13 May 2014	Sinoville	487/04/2013	Handheld skimming. Handheld skimming device. At a merchant in Pretoria.	**	**	**	**		**Joint analysis of positive spend transaction history of different compromised accounts. **Sharing of intelligence and deploying a joint investigation team consisting of bank investigators and SAPS Commercial Crime Unit. **Search of suspect. **Digital forensic examination of skimming device and counterfeit cards.	**Joint data analysis led to merchant being identified as a common point of purchase (common point of compromise). **Arrest, search and seizure. **Victims identified by means of digital forensic examination of skimming device and counterfeit cards.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
43	Gauteng	Sunnyside	850/07/2013	Handheld skimming &	*	*	*	*	*	*Information received re card	*Arrest, search and	*Y	*N	*N	*Y	*N	*N	*Y	*N

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
	Email dated 13 May 2014			ATM mounted skimming. At ATMs (targeting ATM users).			**	**	**	skimming activities and followed up by other SAPS official(s). *Search of suspects and their vehicle. **Interrogation of suspects and following up of information extracted. **Search of suspects' residences. **Digital forensic examination of skimming devices, laptops, personal computer, memory sticks, counterfeit cards and cell phones.	seizure. **Additional seizures. **Victims identified by means of digital forensic examination of skimming devices, computers and counterfeit cards. **Computer software retrieved during digital forensic examination used to encode cards and drive card writers.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
44	Gauteng Email dated 13 May 2014	Wierdabrug	644/10/2013	POS skimming. Portable POS skimming device. Petrol station in Centurion, Gauteng.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect. **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
45	KwaZulu Natal Email dated 15 May 2014	Gingindlovu	325/10/2013	Handheld skimming. Handheld skimming device. At ATM.	**	**	**			*Direct observation by security guard of card skimming activities by suspect. **Information received by SAPS card fraud investigators and followed up. **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
46	KwaZulu Natal Email dated 15 May 2014	Tongaat	67/02/2014	Handheld skimming. Handheld skimming device. At toll booth (Tongaat Plaza).	**	**	**			**Common point of compromise (CPP) positively identified by bank investigator by means of a collective analysis of positive spend transaction history of different compromised accounts.	**Arrest, search and seizure. **94 Victims identified by means of card data (account numbers) retrieved from skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										**Sharing of information between bank investigators and SAPS investigators. **Digital forensic examination of skimming device.									
47	KwaZulu Natal Email dated 15 May 2014	Winterton	21/09/2013	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*	*		*Information received re suspects and followed up by other SAPS official(s). **Digital forensic examination of skimming device, counterfeit cards and cell phone.	*Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device and counterfeit cards.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
48	Limpopo Email dated 16 May 2014	Groblersdal	88/07/2013	Handheld skimming. Handheld skimming device. At petrol station.	**	**	**			**Information of suspect skimming cards followed up. **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
49	Limpopo Email dated 16 May 2014	Malamulele	144/08/2013	Handheld skimming. Handheld skimming device. At ATM (targeting ATM users).	*	*	*			*Information re card skimming followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	*Y **Y	*Y **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
50	Mpumalanga 26/18/2 dated 2012-10-15	Amersfoort	87/08/2012	Handheld skimming. Handheld skimming device. At ATM (targeting ATM users).	*	*	*	*	*	*Information received re card skimming activities received and followed up by other SAPS official(s). *Search of suspects and their vehicle. **Digital forensic examination of skimming device, counterfeit cards and cell phones.	*Arrest, search and seizure. **Victims identified by means of digital forensic examination of skimming device and counterfeit cards.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
51	Mpumalanga 26/18/2 dated 2012-10-15	Delmas	137/04/2012 138/04/2012	Handheld skimming. Handheld skimming device.	**	**	**	**	**	**Information received re card skimming/counterfeit card fraud activities.	**Arrest, search and seizure by joint investigation team	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
				Pump attendants at petrol station.						**Search of suspects and their homes. **Digital forensic examination of skimming devices and counterfeit cards.	consisting of two bank investigators from two different banks and SAPS CCU investigators. **Search of suspects vehicle and homes yielded laptops, counterfeit cards and cash. **Victims identified by means of digital forensic examination of skimming device and counterfeit cards.								
52	Mpumalanga 26/18/2 dated 2012-10-15	Delmas	43/01/2012	Handheld skimming. Handheld skimming device. Bank official working in bank.	**	**	**			**Information received re card skimming activities of clients' cards. **Collective analysis of transaction data of compromised accounts of clients assisted by suspect. **Search of suspect. **Digital forensic examination of skimming device.	**Arrest, search and seizure by joint investigation team consisting of bank investigators and SAPS CCU investigators. **Suspect identified as probable common point of compromise. **No card data found on skimming device.	**Y	**Y	**Y	**Y	**N	**Y	**Y	**Y
53	Mpumalanga 26/18/2 dated 2012-10-15	Ermelo	9/05/2012	Handheld skimming. Handheld skimming device. Pump attendant at petrol station.	**	**	**	**	**	**Information received re card skimming/counterfeit card fraud activities. **Search of suspect and his home. **Digital forensic examination of skimming devices.	**Arrest, search and seizure by joint investigation team consisting of two bank investigators from two different banks and a SAPS CCU investigator. **Search of suspect's home yielded more counterfeit cards, another skimming device, a card encoder and laptop. **Victims identified by	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
											means of digital forensic examination of skimming device.								
54	Mpumalanga 26/18/2 dated 2012-10-15	Ermelo Amersfoort	217/02/2012 87/08/2012	Handheld skimming. Handheld skimming device. At ATM (targeting ATM users).	*	*	*			*Information re card skimming activities received and followed up by other SAPS official(s). *Search of suspect. **Digital forensic examination of skimming device. **Call data analysis of suspects' cell phone call data.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of digital forensic examination of skimming device. **Suspects positively linked to another case (Amersfoort CAS 87/08/2012) by SABRIC using call data analysis.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
55	Mpumalanga 26/18/2 dated 2012-10-15	Hendrina	68/04/2012	Handheld skimming. Handheld skimming device. At ATM (targeting ATM users) & inside bank (bank official).	*	*	*			*Information re card skimming activities received and followed up by other SAPS official(s). *Search of suspect. **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of digital forensic examination of skimming device. **Bank official identified as additional point of compromise by means of collective analysis of account opening documents and transaction history of compromised accounts.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
56	Mpumalanga 26/18/2 dated 2012-10-15	Kabokweni	138/08/2012	Unknown (no skimming device was seized)	**	**		**	**	**Information received re card skimming/counterfeiting activities. **Search of suspect's home. **Digital forensic examination of card encoder, computer, flash drives and counterfeit cards.	**Arrest, search and seizure. **Victims identified by means of digital forensic examination of counterfeit cards	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
57	Mpumalanga 26/18/2 dated	Mbuzini Nelspruit	13/01/2012 309/03/2012	Handheld skimming. Handheld skimming	*	*		*		*Information re card skimming activities, suspect's	*Arrest, search and seizure of a stolen bank	*Y **Y	*Y **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
	2012-10-15			device. At ATM (targeting ATM user).						vehicle registration number and fraudulent withdrawals received and followed up by other SAPS official(s). *Victim identified point of fraudulent spend from sms received from bank re fraudulent withdrawal. *Search of suspect's vehicle. **DNA analysis of stolen card. **Digital forensic examination of stolen bank card found in vehicle. **Camera surveillance footage. **Cell phone call data analysis.	card by other SAPS official(s). *Stolen bank card linked to theft case. **Card holder (victim) of stolen card identified. **Suspect positively linked to stolen card by means of DNA analysis. **153 Fraudulent spend transactions (payments at toll booths) by different suspects identified from an anlysis of negative spend transaction data on bank statement. **Additional suspects identified by means of camera surveillance footage recorded at toll booths. **Positive links between suspects based on cell phone call data analysis.								
58	Mpumalanga 26/18/2 dated 2012-10-15	Middelburg	309/10/2011	Handheld skimming. Handheld skimming device. Cashiers in coffee shop.	**	**	**	**		**Information received re card skimming activities. **Common point of compromise (CPP) positively identified by means of a collective analysis of positive spend transaction history of different compromised accounts. **Search of cashiers. **Digital forensic examination of skimming device and counterfeit card(s). **Search of suspects' homes.	**Arrests, search and seizure by joint investigation team consisting of 3 bank investigators from two banks and SAPS CCU investigators. **Victims identified by means of digital forensic examination of skimming device and counterfeit cards. **Search of homes did not yield any results.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
59	Mpumalanga 26/18/2 dated 2012-10-15	Middelburg	391/12/2011	Handheld skimming. Handheld skimming device. Pump attendant at petrol station.	**	**	**			**Information received re card skimming activities. **Search of suspect's locker. **Digital forensic examination of skimming device and cell phone.	**Arrest, search and seizure. **Victims identified by means of digital forensic examination of skimming device. **PIN numbers identified on documents in locker.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
60	Mpumalanga 26/18/2 dated 2012-10-15	Ogies	126/03/2012	Handheld skimming. Handheld skimming device. Bank official working in bank.	*	*	*	*		*Information re card skimming activities received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) found on skimming device during digital forensic examination of skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
61	Mpumalanga 26/18/2 dated 2014-05-15	Secunda	195/06/2013	Handheld skimming. Handheld skimming device. At petrol station in Secunda.	**	**	**	**		**Information shared by bank investigator with SAPS investigators. **Digital forensic examination of skimming device, counterfeit cards and cell phones.	**Arrest, search and seizure by joint SAPS/bank investigation team. **Victims identified by means of card data (account numbers) retrieved from skimming device and counterfeit cards.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
62	Mpumalanga 26/18/2 dated 2014-05-15	Volksrust	68/04/2013	Handheld skimming. Handheld skimming device. At point of sale inside shop (Volksrust).	**	**	**	**		**Common point of compromise (CPP) positively identified by bank investigator by means of a collective analysis of positive spend transaction history of different compromised accounts. **Sharing of information between bank investigator and SAPS investigators.	**Arrest, search and seizure by joint SAPS/bank investigation team. **Victims identified by means of card data (account numbers) retrieved from skimming device and counterfeit cards.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										**Digital forensic examination of skimming device and counterfeit cards.									
63	Mpumalanga 26/18/2 dated 2012-10-15	Witbank	628/04/2012	Handheld skimming. Handheld skimming device. Cashier in casino.		*	*			*Real-time camera surveillance by casino personnel. **Digital forensic examination of skimming device and cell phone.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of digital forensic examination of skimming device.	*Y **Y	*Y **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
64	Mpumalanga Witbank CAS 361/11/2012 dated 2012-11-13	Witbank	361/11/2012	Handheld skimming. Handheld skimming device. At ATM (targeting card holders using ATM).	**	**	**	**		**Common point of compromise (CPP) (ATM) positively identified by means of a collective analysis of positive spend transaction history of different compromised accounts. **CPP verified by means of information re unsolicited help offered to clients at ATM. **Surveillance of identified ATMs **Digital forensic examination of counterfeit cards.	**Arrests, search and seizure by joint investigation team consisting of 3 bank investigators from two banks, a secutiy company and SAPS CCU investigator. **Victims identified by means of digital forensic examination of counterfeit cards.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
65	North West Email dated 19 May 2014	Coligny	84/05/2013	Handheld skimming. Handheld skimming device. At petrol station in Coligny.	*	*	*			*Information received re card skimming activities and followed up by other SAPS officials. *Search of suspect. **Digital forensic examination of skimming device.	*Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
66	North West Email dated 19 May 2014	Jouberton	84/08/2013	Unknown	**	**		**	**	**Digital forensic examination of card encoder, laptop and counterfeit cards.	**Victims identified by means of card data (account numbers) retrieved from counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
67	North West	Jouberton	69/04/2012	Handheld skimming.	*	*	*			*Information re card	*Arrest, search and	*Y	*N	*N	*Y	*N	*N	*Y	*N

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
	Email dated 9 October 2012			Handheld skimming device. POC unknown.						skimming followed up by other SAPS official(s). **Digital forensic examination of skimming device.	seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
68	North West Email dated 9 October 2012	Klerksdorp	632/03/2012	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users).	*	*	*			*Information re card skimming followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
69	North West Email dated 19 May 2014	Potchefstroom	298/10/2013	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users) in Potchefstroom.	**	**	**	**	**	**Physical undercover surveillance of ATM. **Digital forensic examination of skimming devices and counterfeit cards. **Digital forensic examination of cell phones and call data analysis.	**Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming devices and counterfeit cards during digital forensic examination. **Positive links made between suspects based on call data analysis.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
70	North West Email dated 19 May 2014	Rustenburg	824/05/2013	Handheld skimming. Handheld skimming device. At ATMs (targeting ATM users) in Rustenburg.	**	**	**	**		**Physical undercover surveillance of ATM. **Digital forensic examination of skimming device and counterfeit cards.	**Arrest, search and seizure. **Victims identified whose cards had been compromised by means of card data (account numbers) retrieved from skimming device and counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
71	North West Email dated 19 May 2014	Tlhabane	34/10/2013	Handheld skimming. Handheld skimming device.	**	**	**			**Digital forensic examination of skimming device.	**Victims identified by means of card data (account numbers)	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized: Skimming device(s)	Exhibits seized: Counterfeit card(s)	Exhibits seized: Other relevant equipment	Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
				POC unknown.							retrieved from skimming device during digital forensic examination.								
72	Northern Cape Report dated 15 October 2012	Pampierstat	05/11/2011	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*			*Information followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure. **Victims identified by means of card data (account numbers) retrieved from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
73	Western Cape Email dated 16 October 2012	Atlantis	132/08/2012	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*	*		*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victim(s) identified by means of skimmed card data (account number(s)) downloaded from skimming device(s).	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
74	Western Cape Email dated 16 October 2012	Cape Town Central	85/02/2011	Handheld skimming. Handheld skimming device. At a pub in Cape Town.	*	*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victim(s) identified by means of skimmed card data (account number(s)) downloaded from skimming device(s).	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
75	Western Cape Email dated 20 May 2014	Cape Town Central	219/06/2013	Handheld skimming. Handheld skimming devices. At restaurant in Cape Town.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspects. **Digital forensic examination of skimming devices.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming devices.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
76	Western Cape Email dated 20 May 2014	Cape Town Central	1995/01/2014	Handheld skimming. Handheld skimming devices. At restaurant in Cape Town.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect. **Digital forensic examination	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
										of skimming device and cell phone.	device during digital forensic examination.								
77	Western Cape Email dated 20 May 2014	Cape Town Central	833/03/2014	Handheld skimming. Handheld skimming devices. At restaurant in Cape Town.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect. **Digital forensic examination of skimming device and cell phone.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
78	Western Cape Email dated 20 May 2014	Claremont	215/03/2014	Handheld skimming. Handheld skimming devices. At restaurant in Claremont.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect. **Digital forensic examination of skimming device and cell phone.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
79	Western Cape Email dated 16 October 2012	Milnerton	138/10/2012	Handheld skimming. Handheld skimming device. Coffee shop in Cape Town.	*	*	*	*	**	*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Search of suspect's house. **Digital forensic examination of skimming device, counterfeit cards, computer and cell phones .	*Arrest(s), search and seizure by other SAPS official(s). **Computer seized in suspect's house. **Victims identified by means of skimmed card data (account number(s)) downloaded from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
80	Western Cape Email dated 16 October 2012	Parow	100/07/2011	Handheld skimming. Handheld skimming device. At petrol station (targeting card holders paying for fuel).	*	*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest, search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming device.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
81	Western Cape Email dated 16 October 2012	Somerset West	211/07/2012	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victim(s) identified by means of skimmed card data (account	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized: Skimming device(s)	Exhibits seized: Counterfeit card(s)	Exhibits seized: Other relevant equipment	Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
											number(s)) downloaded from skimming device(s).								
82	Western Cape Email dated 20 May 2014	Table Bay Harbour	53/12/2013	Handheld skimming. Handheld skimming devices. POC unknown.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect and his residence. **Digital forensic examination of skimming device.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on counterfeit cards during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
83	Western Cape Email dated 20 May 2014	Table Bay Harbour	198/01/2014	Handheld skimming. Handheld skimming devices. At restaurant in Table Bay.	**	**	**		**	**Information received re card skimming activities and followed up. **Search of suspect and his residence. **Digital forensic examination of skimming device and cell phone.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device during digital forensic examination. **Positive links with other suspects established by means of cell phone call data analysis.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y
84	Western Cape Email dated 16 October 2012	Woodstock	515/05/2012	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victims identified by means of skimmed card data (account numbers) downloaded from skimming devices.	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y
85	Western Cape Email dated 16 October 2012	Woodstock	621/06/2012	Handheld skimming. Handheld skimming device. POC unknown.	*	*	*			*Information re card skimming/ counterfeit card fraud received and followed up by other SAPS official(s). **Digital forensic examination of skimming device.	*Arrest(s), search and seizure by other SAPS official(s). **Victim(s) identified by means of skimmed card data (account number(s)) downloaded from skimming device(s).	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y	*N **Y	*Y **Y	*N **Y

No	Province & SAPS report reference number and date	Station	CAS no	Method of skimming, Type of skimming device & Point of compromise (POC)	Case situation/background, identification related activities and identification methods used in the case (Prior to investigation indicated with * and during investigation indicated with ** Below 'other SAPS official(s)' means not the investigating officer)							Were the objectives of identification and individualisation achieved? (Yes = Y; No = N; Prior to investigation indicated with * and during investigation indicated with **)							
					Information received/collected re card skimming/ counterfeit card fraud	Suspect(s) arrested/ in custody	Exhibits seized			Identification related activities and methods used	Outcome	Situation	Victim	Witness	Perpetrator (culprit)	Imprint	Origin	Action	Cumulative
							Skimming device(s)	Counterfeit card(s)	Other relevant equipment										
86	Western Cape Email dated 20 May 2014	Woodstock	342/02/2014	Handheld skimming. Handheld skimming devices. At petrol station in Woodstock.	**	**	**			**Information received re card skimming activities and followed up. **Search of suspect. **Digital forensic examination of skimming device and cell phone.	**Arrest, search and seizure. **Victims identified by means of skimmed card data found on skimming device during digital forensic examination.	**Y	**Y	**Y	**Y	**Y	**Y	**Y	**Y

ANNEXURE G: SABRIC TACTICAL WEEKLY PROVINCIAL COMMERCIAL CRIME RISK FORECAST 23/2013 FOR GAUTENG FOR THE PERIOD 23 JUNE 2013 TO 29 JUNE 2013

sabric
Making South African banking safe, secure and fraud free

Tactical Weekly Provincial Commercial Crime Risk Forecast 23/2013

Gauteng

Date: Forecast for period 23 June 2013 to 29 June 2013

Specified purpose

The aim of this document is to focus scarce crime combat resources towards areas where the chances of success can be optimised. Any enquiries regarding this product, or facts contained therein, may be forwarded to email ccc@sabric.co.za

Terms of use

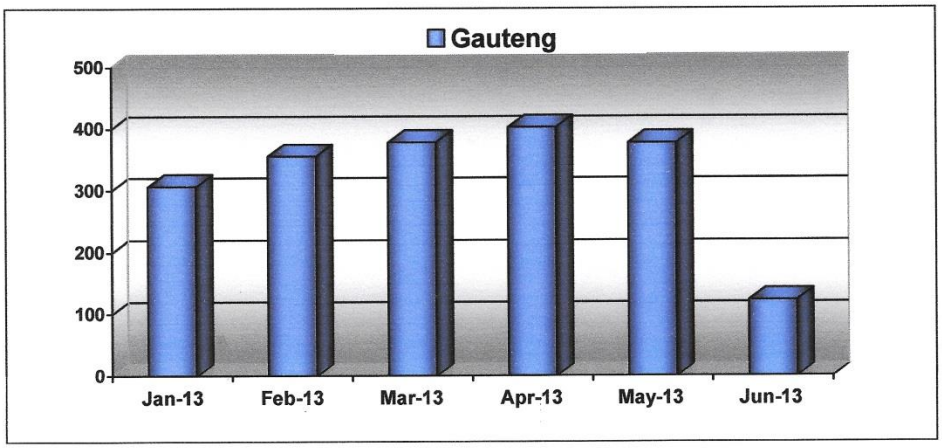
SABRIC's e-mail disclaimer [https://www.sabric.co.za/home.asp?pid=792] is incorporated in these terms and conditions. If you are unable to access the disclaimer, notify us accordingly [CCC@sabric.co.za] and we will send you a copy thereof. The information in this document is confidential and/or protected by law. Although reasonable precautions have been taken, the company cannot guarantee or warrant the accuracy, completeness or fitness of the information contained herein for the purpose specified above. The intended addressee will: 1) use it fairly, lawfully, at his/her own risk and exclusively for the specified purpose; 2) protect it by reasonable measures against loss; unauthorised access, use, modification and disclosure; 3) notify SABRIC of corrections; and 4) destroy the information if it no longer serves the said purpose. SABRIC will not be liable for any damage or loss, relating to the use of the information, whether it arises out of contract or delict, and regardless of whether the possibility of such damage or loss was advised, or not. If you disagree with any of the terms and conditions, you should refrain from using the information and notify SABRIC, without any delay.

Document compiled by: CCO RI Data Administrators

Document reviewed by: CCO Analysts

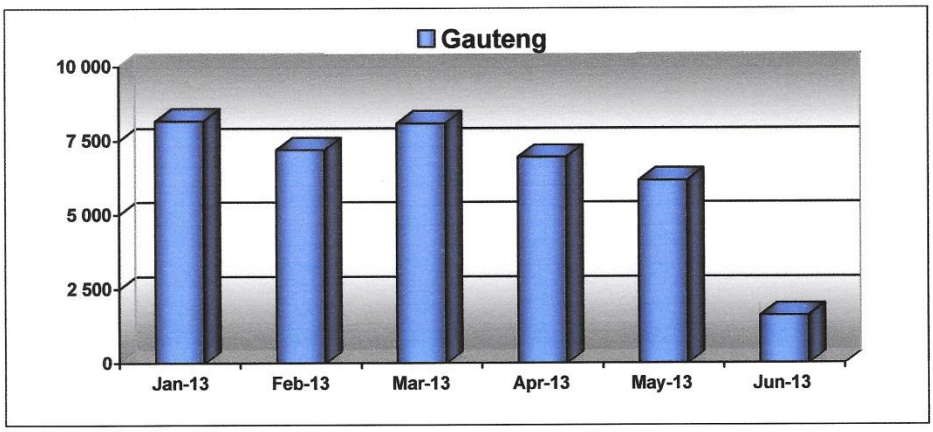
1. PROVINCIAL OVERVIEW

1.1 Cheque Fraud: The graph below provides a running six months overview of the number of cheque fraud incidents within this Province:



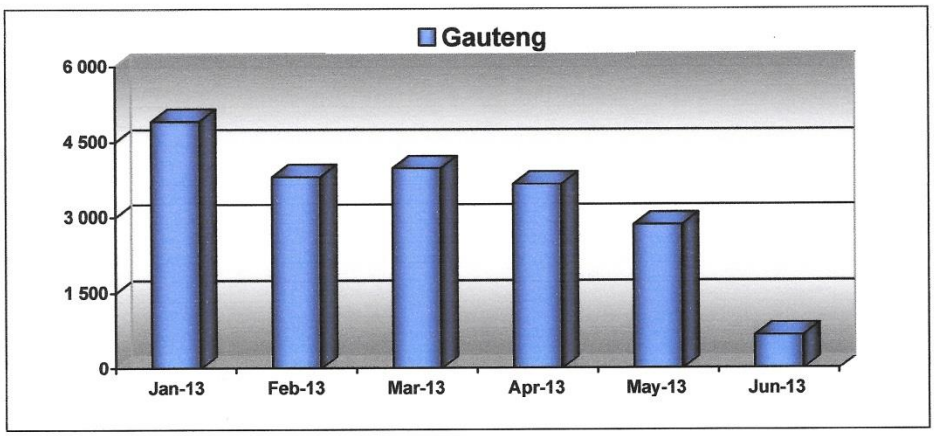
Please note that the data for May and June is not a true reflection of the crime situation as there is a lag time in reporting. These figures will increase as the banks report new identified fraud.

1.2 Credit Card Fraud: The graph below provides a running six months overview of the number of fraudulent credit card transactions within this Province:



Please note that the data for May and June is not a true reflection of the crime situation as there is a lag time in reporting. These figures will increase as the banks report new identified fraud.

1.3 Debit Card Fraud: The graph below provides a running six months overview of the number of fraudulent debit card transactions within this Province:



Please note that the data for May and June is not a true reflection of the crime situation as there is a lag time in reporting. These figures will increase as the banks report new identified fraud.

2. HIGH RISK TOWNS

2.1 LEGEND: Threat Level Colour Codes and Descriptions

Red	The threat is projected to occur in the coming week (forecast for period)
Amber	The threat is projected to occur in the next two weeks.
Blue	The projected threat did not occur in the previous week (week before the forecast for period). A state of alert should still be maintained.

2.2 Fraudulent Cheque Onslaught Forecast

City	Cheque Threat Level
Alberton	Red
Lenasia	Red
Vereeniging	Amber
Westonaria	Amber
Vanderbijlpark	Blue

2.3 Fraudulent Credit Card Onslaught Forecast

City	Credit Card Threat Level
Brakpan	Red
Tokoza	Amber
Katlehong	Amber
Germiston	Amber
Tembisa	Amber

3. GEOGRAPHICAL FOCUS POINTS (Merchants historically targeted)

3.1 Primary Merchants targeted by cheque fraudsters over the last six months:

3.2 Primary Merchants targeted by credit card fraudsters over the last six months:

4. THREAT PERSONA REPORTED IN THE PROVINCE

4.1 Provincial Back of Cheque Information:

Fraud Date	Best Fraud Province	Best Fraud City	BOC ID No	BOC Surname	BOC Cell1

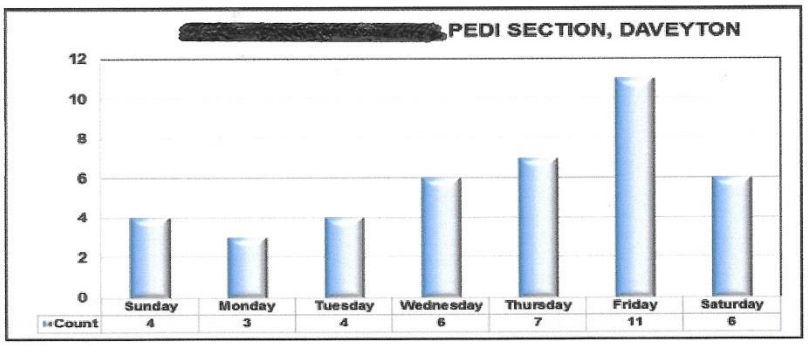
5. ATM HOTSPOTS

The graphs below indicate the top five high risk ATM's within the Gauteng province where withdrawals were made after the card was compromised (**not necessarily the point of compromise**).

The graphs will contain information on the name and location of the ATM as well as the number of incidents per day of the week and hour of the day. This information can be utilised in the planning of possible operations to arrest the criminals while making fraudulent withdrawals at the ATM's.

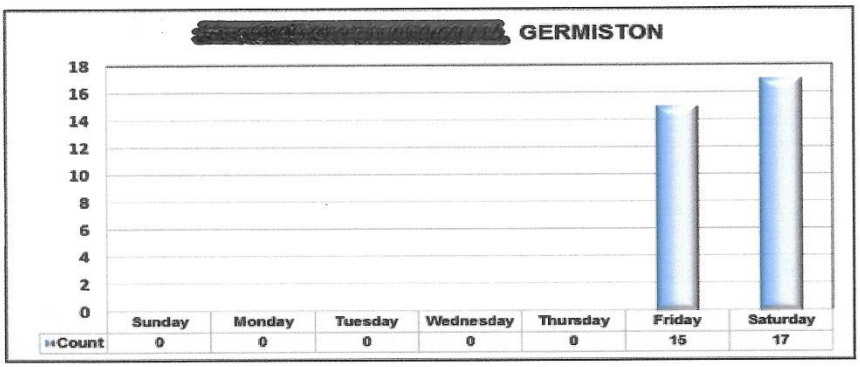
This information will be updated in the tactical weekly on a bi-weekly basis.

ATM 1:



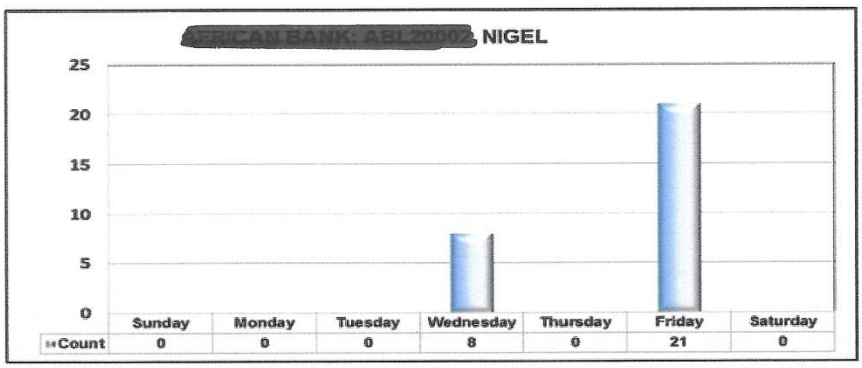
Time of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-01:59	2	0	2	6	6	3	1
02:00-03:59	0	0	0	0	0	0	0
04:00-05:59	0	1	0	0	1	4	3
06:00-07:59	0	0	0	0	0	0	0
08:00-09:59	0	0	0	0	0	1	0
10:00-11:59	0	0	0	0	0	0	0
12:00-13:59	0	0	0	0	0	1	0
14:00-15:59	0	0	0	0	0	0	0
16:00-17:59	0	0	0	0	0	0	0
18:00-19:59	1	0	0	0	0	2	1
20:00-21:59	0	0	0	0	0	0	0
22:00-23:59	1	2	2	0	0	7	1
Unknown	0	0	0	0	0	0	0

ATM 2:



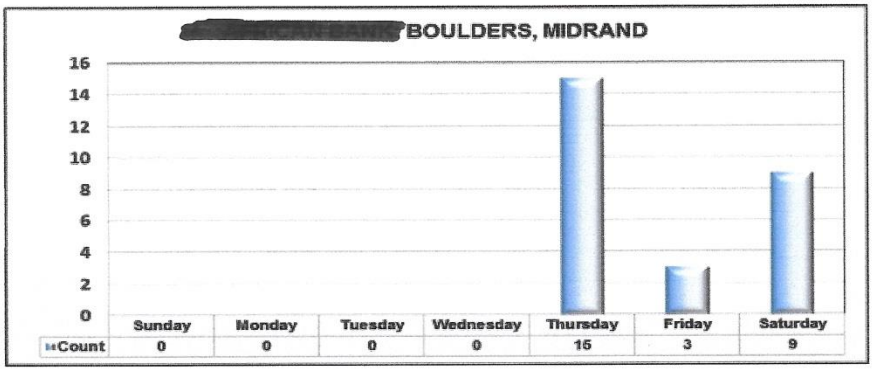
Time of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-01:59	0	0	0	0	0	0	0
02:00-03:59	0	0	0	0	0	0	0
04:00-05:59	0	0	0	0	0	0	0
06:00-07:59	0	0	0	0	0	0	0
08:00-09:59	0	0	0	0	0	0	14
10:00-11:59	0	0	0	0	0	0	3
12:00-13:59	0	0	0	0	0	15	0
14:00-15:59	0	0	0	0	0	0	0
16:00-17:59	0	0	0	0	0	0	0
18:00-19:59	0	0	0	0	0	0	0
20:00-21:59	0	0	0	0	0	0	0
22:00-23:59	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

ATM 3:



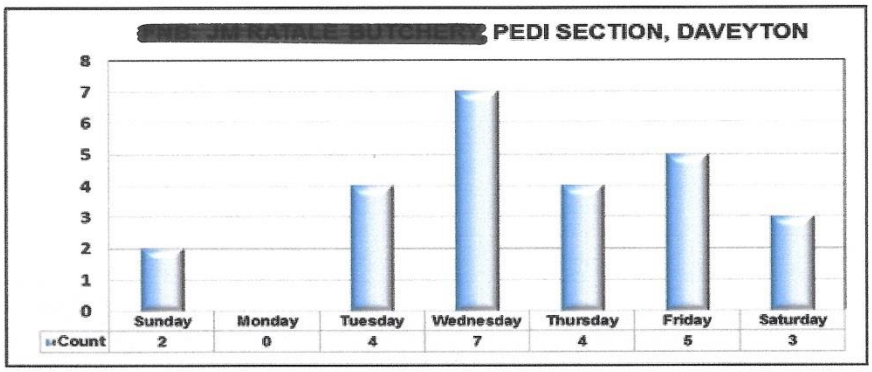
Time of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-01:59	0	0	0	0	0	0	0
02:00-03:59	0	0	0	0	0	0	0
04:00-05:59	0	0	0	0	0	0	0
06:00-07:59	0	0	0	8	0	0	0
08:00-09:59	0	0	0	0	0	0	0
10:00-11:59	0	0	0	0	0	0	0
12:00-13:59	0	0	0	0	0	0	0
14:00-15:59	0	0	0	0	0	0	0
16:00-17:59	0	0	0	0	0	8	0
18:00-19:59	0	0	0	0	0	13	0
20:00-21:59	0	0	0	0	0	0	0
22:00-23:59	0	0	0	0	0	2	0
Unknown	0	0	0	0	0	0	0

ATM 4:



Time of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-01:59	0	0	0	0	0	0	0
02:00-03:59	0	0	0	0	0	0	0
04:00-05:59	0	0	0	0	0	0	0
06:00-07:59	0	0	0	0	0	0	0
08:00-09:59	0	0	0	0	0	0	0
10:00-11:59	0	0	0	0	0	0	0
12:00-13:59	0	0	0	0	0	0	0
14:00-15:59	0	0	0	0	0	0	0
16:00-17:59	0	0	0	0	0	3	9
18:00-19:59	0	0	0	0	15	0	0
20:00-21:59	0	0	0	0	0	0	0
22:00-23:59	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

ATM 5:



Time of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-01:59	0	0	0	0	0	0	0
02:00-03:59	0	0	0	0	0	0	0
04:00-05:59	0	0	0	0	0	0	0
06:00-07:59	0	0	0	3	2	2	2
08:00-09:59	0	0	2	0	1	1	1
10:00-11:59	1	0	0	0	0	0	0
12:00-13:59	1	0	0	0	0	2	0
14:00-15:59	0	0	1	3	1	0	0
16:00-17:59	0	0	1	1	0	0	0
18:00-19:59	0	0	0	0	0	0	0
20:00-21:59	0	0	0	0	0	0	0
22:00-23:59	0	0	0	0	0	0	0
Unknown	0	0	0	0	0	0	0

INCIDENTS

Crime incidents reported to SABRIC for the period 20 May 2013 to 20 June 2013

Inc Reg	SAPS CAS	Date	Crime Type	Instrument	Method	Financial Onslaught	Suburb	Town	Province
Persona ID	**Persona Arrested**	**Persona ID**	**Telephone No**	**Arrest Date**	**Aliases**	**Possibly Related Cases**	**Links Available Y/N**	**IO Details**	**Photo**

ANNEXURE H: CRIME PATTERN ANALYSIS AND CRIME MAPS RELATING TO FRAUD INCIDENTS REGISTERED AT SAPS DAVEYTON, COMMITTED DURING THE PERIOD 1 TO 30 JUNE 2013, AND 23 TO 29 JUNE 2013 RESPECTIVELY, COMPILED WITH THE SAPS GEOGRAPHIC INFORMATION SYSTEM

17/4/2014

2014-04-17 09:58
10.100.238.147

sapsprd:9000/pls/intprd/GISYPCKCPAANALYST.cpa

Geographic Information System

Level	Station
Component	Daveyton
Category	All (A+B)
Offence Group	(Dasc23) Fraud
Date Type	Committed
Begin Date	2013-06-01
End Date	2013-06-30

Quick Filter | Open with Spreadsheet | Show Map | Save Result | Full Matrix

* UKN - Abbreviation for Unknown

	Offence Data																Victim Data				Complainant Data							
Pin No.	Component	Case No.	Complaint No.	Offence	Day of Month (Begin)	Day of Month (End)	Day of Week	Time (Begin)	Time (End)	Place	Street	Street No.	Suburb	CAS Block	X-Coord	Y-Coord	Method	Instrument	Race	Gender	Age	Name	Race	Gender	Age	Name	No.of Accused	Race	Gender	Nat
1	Daveyton	71/10/2013	1	Fraud	2013-06-01	2013-06-30	Saturday	09:00	17:00	UKN	Russels Furniture Daveyton Mall	UKN	Sotho	6440	28.41893822	-26.15480802	Forge Signature	Unknown	UKN	UKN	UKN	UKN	Black	Female	43	Thobeka Dlali	0	UKN	UKN	UKN
2	Daveyton	104/6/2013	1	Fraud	2013-06-04	2013-06-04	Tuesday	08:00	08:00	Daveyton Mall	Eiselen And Turton	UKN	Basotho	6440	28.41711516	-26.15609197	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	55	Agnes Thoni Moshane	0	UKN	UKN	UKN
3	Daveyton	178/6/2013	1	Fraud	2013-06-04	2013-06-04	Tuesday	21:00	21:00	Majuteni Shopping Complex Absa Atm	Maroleng Street	UKN	Basotho	6440	28.42855285	-26.1511852	Withdraw Money	Bank Card	UKN	UKN	UKN	UKN	White	Male	43	Daniel Themba Ndlovu	0	UKN	UKN	UKN
4	Daveyton	91/6/2013	1	Fraud	2013-06-05	2013-06-05	Wednesday	08:40	08:40	Ratala Butchery	Lobedu	UKN	Basotho	6440	28.42568584	-26.14469657	Forge	Unknown	UKN	UKN	UKN	UKN	Black	Male	43	Sello Hamilton Maboke	0	UKN	UKN	UKN
5	Daveyton	450/6/2013	1	Fraud	2013-06-07	2013-06-08	Friday	07:00	12:00	Shoprite Sesfikile Mall	Heald Str (Daveyton Rd)	UKN	Tsonga	6440	28.4245564	-26.1444356	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	35	Glory Sithole	0	UKN	UKN	UKN
6	Daveyton	170/6/2013	1	Fraud	2013-06-07	2013-06-07	Friday	15:41	15:41	UKN	Daveyton	UKN	Daveyton	6440	28.42525765	-26.14557514	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	41	Selina Babeleni Masilela	0	UKN	UKN	UKN
7	Daveyton	344/6/2013	1	Fraud	2013-06-08	2013-06-09	Saturday	08:00	08:00	UKN	Horwood Street	1	Secunda	6440	28.41606977	-26.1450492	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	54	Mkhetwa Malawi Doctor Mahlangu	0	UKN	UKN	UKN
8	Daveyton	396/12/2013	1	Fraud	2013-06-08	2013-06-08	Saturday	15:00	15:00	UKN	Mabaso	UKN	Central	6428	28.4249141	-26.1405689	Take	Hands	UKN	UKN	UKN	UKN	Black	Male	43	Conrad Mphahlele	1	Black	Male	R S A
9	Daveyton	343/6/2013	1	Fraud	2013-06-09	2013-06-09	Sunday	11:00	18:00	UKN	None	UKN	Daveyton	6440	28.72334358	-25.82516931	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	47	Sophie Veni Mahlangu	0	UKN	UKN	UKN
10	Daveyton	368/2/2014	1	Fraud	2013-06-10	2013-06-20	Monday	09:00	09:00	Daveyton Mall Nedbank	Eiselen Street	UKN	Daveyton	6440	28.41725622	-26.15395561	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	54	Marcelle Johannes Maloma	0	UKN	UKN	UKN
11	Daveyton	302/6/2013	1	Fraud	2013-06-13	2013-06-13	Thursday	16:20	16:20	Daveyton Mall	Eiselen Street	UKN	Daveyton	6440	28.41619	-26.14863295	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	38	Soutman Joseph Ramokoatsi	0	UKN	UKN	UKN
12	Daveyton	520/6/2013	1	Fraud	2013-06-15	2013-06-23	Saturday	17:00	11:49	Absa Bank Daveyton Mall	Eiselen Street	UKN	Basotho	6440	28.42560828	-26.14478622	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	57	Sebenzani Nzalina Nhlabati	0	UKN	UKN	UKN
13	Daveyton	348/6/2013	1	Fraud	2013-06-16	2013-06-16	Sunday	17:55	17:55	Zok	Eiselen Street	UKN	Daveyton	6440	28.42604657	-26.14496154	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	White	Female	13	Cleriza Pretorius	0	UKN	UKN	UKN
14	Daveyton	84/7/2013	1	Fraud	2013-06-18	2013-06-18	Tuesday	08:00	08:00	UKN	Cnr Eiselen Street And Turton Street	UKN	Daveyton	6440	28.41711516	-26.15609197	Withdraw Money	Bank Card	UKN	UKN	UKN	UKN	Black	Female	61	Tobi Agnes Baloyi	0	UKN	UKN	UKN
15	Daveyton	319/6/2013	1	All Other Fraud And Related Offences	2013-06-18	2013-06-18	Tuesday	10:00	10:00	UKN	UKN	UKN	UKN	6442	28.40612717	-26.16104129	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	54	Jeffrey Maisba	0	UKN	UKN	UKN
16	Daveyton	523/6/2013	1	Fraud	2013-06-19	2013-06-19	Wednesday	09:00	09:00	Capitec Bank Atm	Eiselen Str	UKN	Daveyton	6440	28.42341685	-26.14408497	Withdraw Money	Electronic Card Reader	UKN	UKN	UKN	UKN	Black	Male	48	David Tsikane Obcletswe	0	UKN	UKN	UKN
17	Daveyton	367/6/2013	1	Fraud	2013-06-21	2013-06-21	Friday	07:15	07:15	UKN	UKN	UKN	UKN	6440	28.42240271	-26.14809847	Withdraw Money	Bank Card	UKN	UKN	UKN	UKN	Black	Male	25	Wilson Meleji	0	UKN	UKN	UKN
18	Daveyton	440/6/2013	1	Fraud	2013-06-21	2013-06-24	Friday	08:00	09:15	UKN	Heald	UKN	UKN	6440	28.40102041	-26.1627177	Withdraw Money	Hands	UKN	UKN	UKN	UKN	Black	Male	45	Bongani Cyprian Zikubu	0	UKN	UKN	UKN
19	Daveyton	518/6/2013	1	Fraud	2013-06-23	2013-06-23	Sunday	11:45	11:45	UKN	Bronkhorstspruit	UKN	Bronkhorstspruit	6440	28.74775928	-25.80468312	Withdraw Money	Bank Card	UKN	UKN	UKN	UKN	Black	Female	33	Sophie Bongi Mahlangu	0	UKN	UKN	UKN
																										Khotakele				

]

20	Daveyton	403/1/2014	1	Fraud	2013-06-24	2013-06-24	Monday	10:00	10:00	UKN	a Street	1161	Daveyton	6439	28.41282	-26.15008	Forge	Unknown	N	UKN	UKN	UKN	Black	Female	65	Patricia Nkosi Mlambo	0	UKN	UKN	UKN
21	Daveyton	63/7/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	04:32	04:32	Standard Bank	Corner Of Hlakwana	NONE	Daveyton	6440	28.41940564	-26.15167706	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	44	Patience Sosineke Molo	0	UKN	UKN	UKN
22	Daveyton	518/6/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	08:41	08:41	Fnb Bank	Daveyton	UKN	Daveyton	6440	28.42473171	-26.14531217	Take	Unknown	UKN	UKN	UKN	UKN	Black	Female	34	Fortunate Thoko Nkosi	0	UKN	UKN	UKN
23	Daveyton	446/6/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	10:01	10:01	Fnb Atm Saza	Lobedu	UKN	Basotho	6440	28.42297857	-26.14557514	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	37	Evah Siwele	0	UKN	UKN	UKN
24	Daveyton	488/6/2013	1	Fraud	2013-06-27	2013-06-27	Thursday	02:03	02:03	UKN	Sesfikile Shoprite Heald Str	UKN	Ext 2	6442	28.40605847	-26.16108423	Force	Unknown	UKN	UKN	UKN	UKN	Black	Male	23	Wisani Mathebula	0	UKN	UKN	UKN
25	Daveyton	309/7/2013	1	Fraud	2013-06-28	2013-06-28	Friday	15:00	15:00	Absa Atm	Mosane Street	UKN	Daveyton	6440	28.42490702	-26.14496154	Withdraw Money	Cash (Money)	UKN	UKN	UKN	UKN	Black	Male	48	Dick Dickson Mbalukani	0	UKN	UKN	UKN

Quick Filter | Open with Spreadsheet | Show Map | Save Result | Full Matrix

17/4/2014 sapsprd:9000/pls/intprd/GISYPCKCPAANALYST.cpa

2014-04-17 10:00
10.100.238.147

Geographic Information System

Level	Station
Component	Daveyton
Category	All (A+B)
Offence Group	(Disc23) Fraud
Date Type	Committed
Begin Date	2013-06-23
End Date	2013-06-29

Quick Filter | Open with Spreadsheet | Show Map | Save Result | Full Matrix

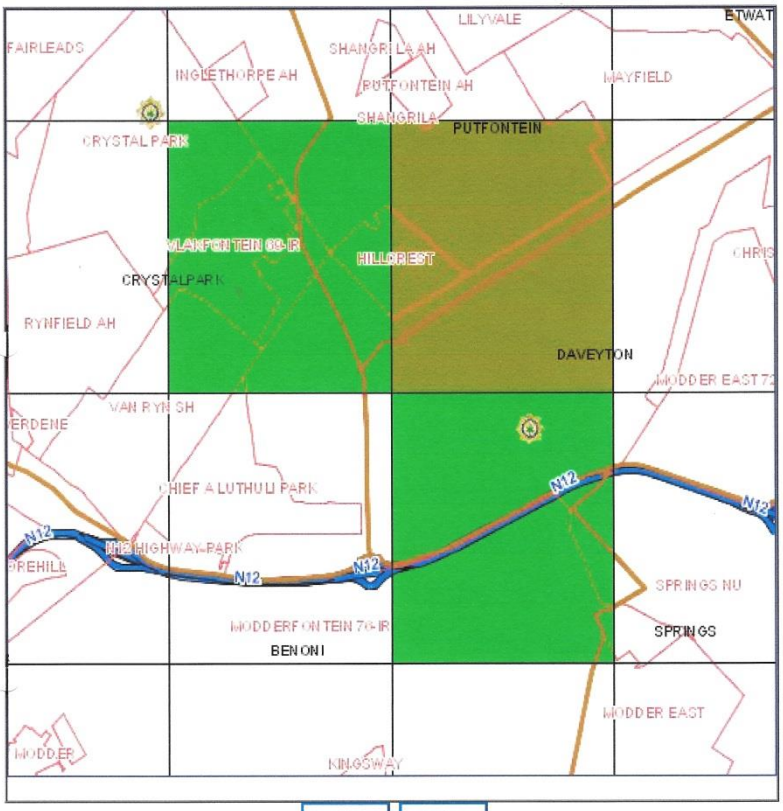
* UKN - Abbreviation for Unknown

					Offence Data												Victim Data				Complainant Data				Accused Data			
Pin No.	Component	Case No.	Complaint No.	Offence	Day of Month (Begin)	Day of Month (End)	Day of Week	Time (Begin)	Time (End)	Place	Street	Street No.	Suburb	CAS Block	X-Coord	Y-Coord	Method	Instrument	Race	Gender	Age	Name	Race	Gender	Age	Name	No.of Accused	Race	Gender	Nationali
1	Daveyton	518/6/2013	1	Fraud	2013-06-23	2013-06-23	Sunday	11:45	11:45	UKN	Bronkhorstepruit	UKN	Bronkhorstepruit	6440	28.74775928	-25.80468312	Withdraw Money	Bank Card	UKN	UKN	UKN	UKN	Black	Female	33	Sophia Bongi Mahlangu	0	UKN	UKN	UKN
2	Daveyton	403/1/2014	1	Fraud	2013-06-24	2013-06-24	Monday	10:00	10:00	UKN	Venda Street	1161	Daveyton	6439	28.41282	-26.15008	Forge	Unknown	UKN	UKN	UKN	UKN	Black	Female	65	Kholakele Patricia Nkosi Mlambo	0	UKN	UKN	UKN
3	Daveyton	63/7/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	04:32	04:32	Standard Bank	Corner Of Hlakwana	NONE	Daveyton	6440	28.41940564	-26.15167706	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Male	44	Patience Sosineke Molo	0	UKN	UKN	UKN
4	Daveyton	518/6/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	08:41	08:41	Fnb Bank	Daveyton	UKN	Daveyton	6440	28.42473171	-26.14531217	Take	Unknown	UKN	UKN	UKN	UKN	Black	Female	34	Fortunate Thoko Nkosi	0	UKN	UKN	UKN
5	Daveyton	446/6/2013	1	Fraud	2013-06-25	2013-06-25	Tuesday	10:01	10:01	Fnb Atm Saza	Lobedu	UKN	Basotho	6440	28.42297857	-26.14557514	Withdraw Money	Unknown	UKN	UKN	UKN	UKN	Black	Female	37	Evah Siwele	0	UKN	UKN	UKN
6	Daveyton	488/6/2013	1	Fraud	2013-06-27	2013-06-27	Thursday	02:03	02:03	UKN	Sesfikile Shoprite Heald Str	UKN	Ext 2	6442	28.40605847	-26.16108423	Force	Unknown	UKN	UKN	UKN	UKN	Black	Male	23	Wisani Mathebula	0	UKN	UKN	UKN
7	Daveyton	309/7/2013	1	Fraud	2013-06-28	2013-06-28	Friday	15:00	15:00	Absa Atm	Mosane Street	UKN	Daveyton	6440	28.42490702	-26.14496154	Withdraw Money	Cash (Money)	UKN	UKN	UKN	UKN	Black	Male	48	Dick Dickson Mbalukani	0	UKN	UKN	UKN

Quick Filter | Open with Spreadsheet | Show Map | Save Result | Full Matrix

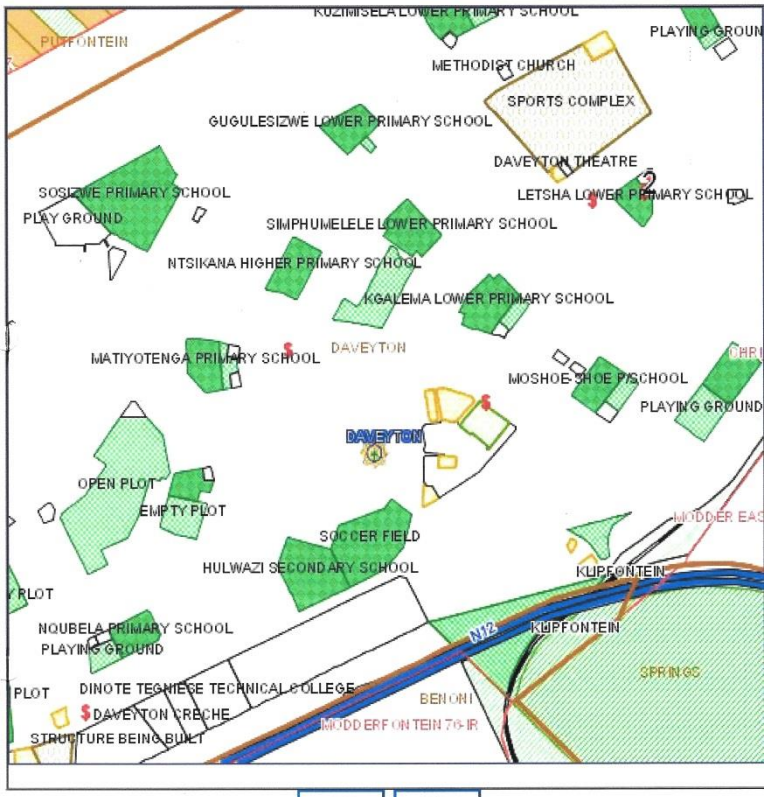
Incident	Component	Case	Offence	Day of Month (Begin)	Day of Month (End)	Day of Week	Time (Begin)	Time (End)	Place Name	Street Name	Street No.	Suburb	CAS Block	X-Coord	Y-Coord	Method Used
25	Daveyton	309/7/2013	Fraud	2013/06/28	2013/06/28	Friday	15:00	15:00	Absa Atm	Mosane Street	UKN	Daveyton	6440	28.42491	-26.145	Withdraw Money
12	Daveyton	520/6/2013	Fraud	2013/06/15	2013/06/23	Saturday	17:00	11:49	Absa Bank Daveyton Mall	Elselen Street	UKN	Basotho	6440	28.42561	-26.1448	Withdraw Money
16	Daveyton	523/6/2013	Fraud	2013/06/19	2013/06/19	Wednesday	09:00	09:00	Capitec Bank Atm	Elselen Str	UKN	Daveyton	6440	28.42342	-26.1441	Withdraw Money
2	Daveyton	104/6/2013	Fraud	2013/06/04	2013/06/04	Tuesday	08:00	08:00	Daveyton Mall	Elselen And Turton	UKN	Basotho	6440	28.41712	-26.1551	Withdraw Money
11	Daveyton	302/6/2013	Fraud	2013/06/13	2013/06/13	Thursday	18:20	18:20	Daveyton Mall	Elselen Street	UKN	Daveyton	6440	28.41819	-26.1486	Withdraw Money
10	Daveyton	368/2/2014	Fraud	2013/06/10	2013/06/20	Monday	09:00	09:00	Daveyton Mall Nedbank	Elselen Street	UKN	Daveyton	6440	28.41726	-26.154	Withdraw Money
23	Daveyton	446/6/2013	Fraud	2013/06/25	2013/06/25	Tuesday	10:01	10:01	Fnb Atm Saza	Lobedu	UKN	Basotho	6440	28.42298	-26.1456	Withdraw Money
22	Daveyton	519/6/2013	Fraud	2013/06/25	2013/06/25	Tuesday	08:41	08:41	Fnb Bank	Daveyton	UKN	Daveyton	6440	28.42473	-26.1453	Take
3	Daveyton	179/6/2013	Fraud	2013/06/04	2013/06/04	Tuesday	21:00	21:00	Majuteni Shopping Complex Absa Atm	Maroleng Street	UKN	Basotho	6440	28.42955	-26.1512	Withdraw Money
4	Daveyton	91/6/2013	Fraud	2013/06/05	2013/06/05	Wednesday	08:40	08:40	Ratale Butchery	Lobedu	UKN	Basotho	6440	28.4257	-26.1447	Forge
5	Daveyton	450/6/2013	Fraud	2013/06/07	2013/06/08	Friday	07:00	12:00	Shoprite Sesfikile Mall	Heald Str (Daveyton Rd)	UKN	Tsonga	6440	28.42456	-26.1444	Withdraw Money
21	Daveyton	63/7/2013	Fraud	2013/06/25	2013/06/25	Tuesday	04:32	04:32	Standard Bank	Corner Of Hlakwana	NONE	Daveyton	6440	28.41941	-26.1517	Withdraw Money
1	Daveyton	71/10/2013	Fraud	2013/06/01	2013/06/30	Saturday	09:00	17:00	UKN	Russels Furniture Daveyton Mall	UKN	Sotho	6440	28.41894	-26.1548	Forge Signature
6	Daveyton	170/6/2013	Fraud	2013/06/07	2013/06/07	Friday	15:41	15:41	UKN	Daveyton	UKN	Daveyton	6440	28.42526	-26.1456	Withdraw Money
7	Daveyton	344/6/2013	Fraud	2013/06/08	2013/06/09	Saturday	08:00	08:00	UKN	Horwood Street	1	Secunda	6440	28.41807	-26.145	Withdraw Money
8	Daveyton	396/12/2013	Fraud	2013/06/08	2013/06/08	Saturday	15:00	15:00	UKN	Mabaso	UKN	Central	6428	28.42429	-26.1406	Take
9	Daveyton	343/6/2013	Fraud	2013/06/09	2013/06/09	Sunday	11:00	18:00	UKN	None	UKN	Daveyton	6440	28.72334	-25.8252	Withdraw Money
14	Daveyton	84/7/2013	Fraud	2013/06/18	2013/06/18	Tuesday	08:00	08:00	UKN	Cnr Elselen Street And Turton Street	UKN	Daveyton	6440	28.41712	-26.1551	Withdraw Money

Crime map (grid): SAPS Daveyton: 23 to 29 June 2013

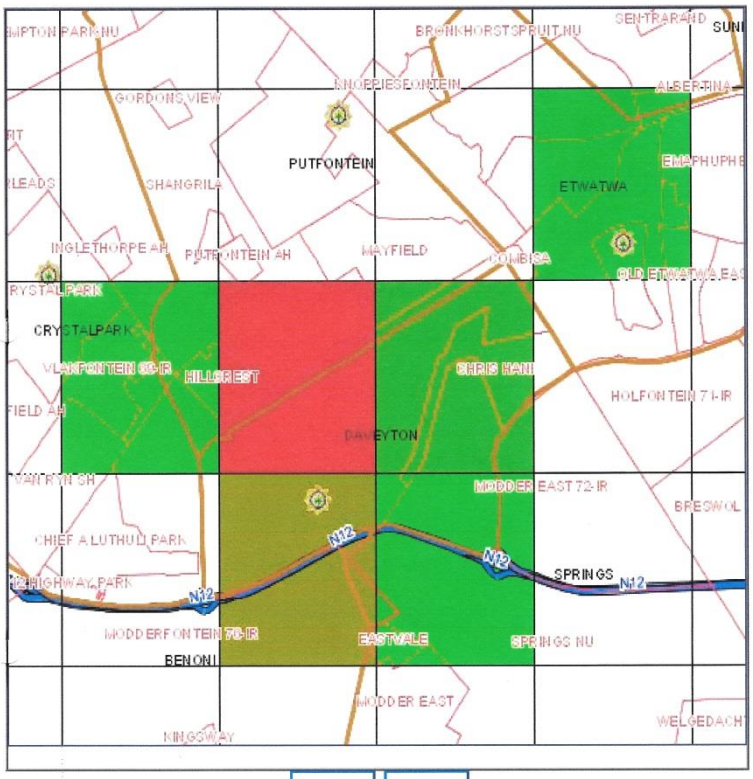


17/4/2014 Global Access Control System - : : Production : :

Crime map: Fraud: SAPS Daveyton: 23 to 29 June 2013

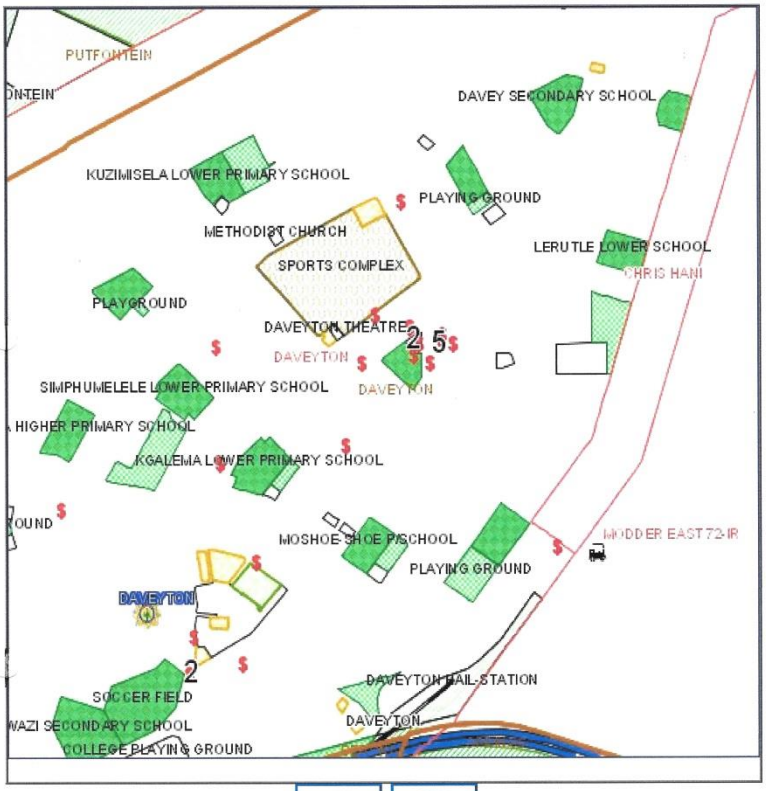


Crime map (grid): SAPS Daveyton: 1 to 30 June 2013



OK PRINT

Crime map: Fraud: SAPS Daveyton: 1 to 30 June 2013



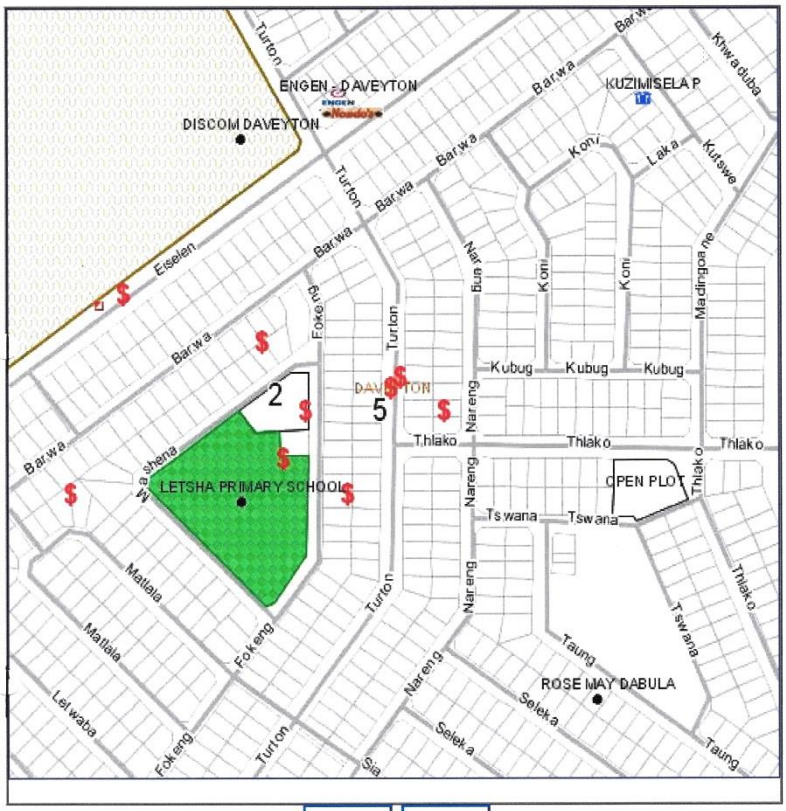
OK PRINT

Fraud hotspots: Daveyton: 1 to 30 June 2013

OK PRINT

17/4/2014 Global Access Control System - : : Production : :

Fraud hotspots: Daveyton: 1 to 30 June 2013



OK PRINT

Fraud hotspots: Daveyton: 1 to 30 June 2013