**Examining the unique security features of a credit card with the aim of identifying possible fraudulent use**

by

**TREVOR BUDHRAM**

**Submitted in part fulfilment of the requirements for the**

**MAGISTER TECHNOLOGIAE**

**In the subject**

**FORENSIC INVESTIGATION**

**at the**

**UNIVERSITY OF SOUTH AFRICA**

**SUPERVISOR: DR N.J.C. OLIVIER**

**September 2007**

**Acknowledgements**

I would like to thank my supervisor, Dr Nick Olivier for the full support, guidance and encouragement that he gave me throughout the entire project. This project succeeded because of your guidance and commitment.

To my wife Ruby, I appreciate the patience, assistance, motivation and encouragement provided throughout the project.

To my daughter Sasha, thank you for the patience shown and respect for my privacy when working on this project.

**Summary**

**Examining the unique security features on a credit card with the aim of identifying possible fraudulent use.**

The use of credit cards has become a way of life in many parts of the world. Credit cards have also created many new opportunities for criminal activity.

It is in this light that organizations such as VISA International have explored a variety of security alternatives by constantly reviewing security measures that may be applied to cards and devote considerable resources to the maintenance of security systems and programmes. These programmes mandated by the association, include uniform card standards, security standards for manufactures, embossing and encoding of cards, standards for mailing the cards and credit background investigations of applicants. These standards assist investigators in examining counterfeit cards and distinguish a counterfeit card from a genuine card. The constant reviewing of security features and methods by the association is to create a card that is technically difficult to alter or counterfeit.

Key Terms:

Fraud, Credit card fraud, Forensic Investigation, Identification, Investigation, Evidence, Locard Principle, Feature, Prevention, Counterfeit.

## TABLE OF CONTENTS

**Heading** **Page number**

**Chapter One: General Orientation**

**Chapter Two: Credit Card Fraud**

**Annexures**

# CHAPTER 1
# GENERAL ORIENTATION

## 1.1 Introduction

Criminals are always looking for the opportunity to commit crime of which the breaking of financial systems, particularly credit cards, is but one. During the low-tech era of the 1980s it was relatively easy to counterfeit credit cards (Visa International Law Enforcement Education Programme, 2000:12). When a credit card is used as an instrument to commit fraud it will contain evidence of misrepresentation and other unlawful changes, which can be identified to prove the crime of fraud.

Criminals used a number of unsophisticated methods like “shave and paste”, a procedure that included carefully shaving off the embossed account numbers from the plastic with a sharp razor blade and then pasting on new account numbers by carefully using special liquid glue. Criminals found this method highly effective because in the days before electronic digital machines for swiping a card was invented, the old paper and machine system, where the card’s numbers are physically imprinted on the credit card slip, were so carefully re-arranged that the numbers were not always picked up by shop assistants. The numbers were then rearranged to match a good account number. Good account numbers included numbers obtained from stolen credit cards and existing card numbers issued by banking institutions. Another method used was “Punching”, a process that required the use of a paper-hole-punch in order to punch each number out from the plastic card by carefully placing the punched numbers in the holes in the plastic to match a good account number. “Re-embossing”, includes a process of placing identifying data on a bank card in the form of raised characters. This is a method of placing a good account number on a stolen or lost card. The process involves firstly flattening the card. Once the card is flattened the good account number can then be embossed over the flattened number.

According to recent statistics released by the South African Banking Risk Information Centre (SABRIC) for the year 2006/01/15 to 2007/01/15 with reference to credit card fraud, there is a 78 per cent increase in the crime nationally in South Africa (SABRIC, Annual Statistics. January 2006 to January 2007. Johannesburg). Statistics compiled by the provincial office of the South African Police Service (SAPS) commercial crime branch, Gauteng for the period 2006/01/15 to 2007/01/15 indicates an 80% increase in credit card fraud of which 50% of the fraud was committed by the manipulation of the unique security features on the credit cards (SAPS, Commercial Branch, Gauteng. Annual Statistics. January 2006 to January 2007. Johannesburg).

The researcher has been involved in criminal investigations for the past eight years of which six-and-a-half years have been devoted to the investigation of fraud-related crimes. During inspections of credit card case dockets, conducted over the past five years and informal lectures presented at the SAPS commercial branches in the Gauteng policing area, as well as the perusal of the training curriculum of corporate investigators and speaking to them on this issue, it has become evident that investigators do not examine the security features, but only concentrate on the signature endorsed on the reverse side of credit cards. This problem, however, originates from the fact that the training curriculum of investigators in the South African Police Service (SAPS) and the corporate sectors do not include any specific training dealing with these unique security features when investigating credit card fraud. Neither has any study material on credit card fraud been incorporated into their respective curricula for presentation in lectures or training workshops. This shortcoming was confirmed by an examination and perusal of the training curricula for investigators in the police and corporate sector.

### 1.2 Aim

The aim of this study was to research the unique security features of credit cards with the aim of identifying possible fraudulent use.

## 1.3 Purpose

Denscombe (2002:25) explains that the purpose of research should be stated clearly and explicitly. The statement of purpose also indicates the focus and directions of the research and provides criteria for the evaluation of the outcome of the research.

The researcher decided on the following purposes:

- To evaluate what the situation with reference to the unique security features of a credit card currently is by identifying strengths and weaknesses and consider how things should be improved (Denscombe, 2002:25). The researcher examined the work of investigators and interviewed them in an attempt to get to the root of the problem with reference to identifying the strengths and weaknesses of investigators in identifying fraudulent security features on credit cards.
- To explore national and international literature in order to find out what the latest investigation trends in this regard are (Denscombe, 2002:25). The purpose of this exploratory research is to collect facts and to report back how things are currently addressed internationally.
- The researcher wishes to develop good practices which will address the problem and enhance the performance of individuals during their daily duties (Denscombe, 2002:25). In his recommendations the researcher will suggest procedures for application in practice that could help to solve the problem regarding the identification of fraudulent security features on credit cards.

## 1.4 Research Questions

Salkind (1997:6) states that a research question is the first and most important step in research which arises as the result of curiosity and it becomes necessary to find an answer. He further states that research questions are informally stated and is often intended as a source of discussion and stimulation about what direction the specific research topic should take.

To research the problem and reach the aims of the research, the researcher decided on the following areas of thematic interest that he envisages addressing in the research (Noak & Wincup, 2004:122):

- What is meant by the concept credit card?
- What are the unique features of a credit card?
- What preventative counter measures can be taken to prevent fraudulent manipulation of the security features on a credit card?

## 1.5 Key Theoretical Concepts

### 1.5.1 Fraud

Fraud is the unlawful and intentional misrepresentation, which results in actual or potential loss (Fischer, 1999:131).

### 1.5.2 Credit Card

A credit card is a Financial Transaction Card that allows the cardholder to obtain money, goods or services under a line of credit established by the card issued (Visa International, 2004:81).

### 1.5.3 Forensic Investigation

Forensic investigation is a process of collecting facts that can serve as evidence before a court of law, through which the associative part of an accused in the commission of a crime can be proved (Slyter, 1995:21).

### 1.5.4 Identification

Identification can be the principle that all objects in the universe are unique because it has certain unique individual or group characteristics. It includes all relevant information, which may shed light on a case and create awareness of the possible value of every potential source of information (Marais, 1992:19).

### 1.5.5 Investigation

Investigation is the systematic search for the truth with the primary purpose of finding a positive solution to the crime with the help of objective and subjective clues (Van der Westhuizen, 1996:01).

### 1.5.6 Evidence

Evidence is defined as anything that tends to prove or disprove a fact in contention (Gardner, 2005:7).

### 1.5.7 Locard Principle

Locard principle is a process whereby whenever two objects come into contact with one another, material from the first would be transferred to the second and material from the second would be transferred to the first (Gardner, 2005:24).

## 1.6 Research Design

A research design is the complete strategy of attack on the central research problem (Leedy & Ormrod, 2001:91). The reason for a research design is that it provides the overall structure for the procedures that a researcher follows, the data that the researcher collects and the data analysis that the researcher conducts (Leedy & Ormrod, 2001:91). The research design to be adopted in this study is of an empirical nature. The researcher decided on this because of the fact that there is very little information in the literature that could answer the research questions posed and therefore he has had to produce new knowledge by using the experience of investigators and gathering information from practice (Denscombe, 2002:6). The researcher is of the opinion that an empirical design has to be employed to get information from participants because of their experience. Maxfield and Babbie (1995:4) explain empirical design to be production of knowledge based on experience and observation.

For the purpose of this research a qualitative research approach was used. Qualitative study is exploratory in nature which allows the researcher to listen and

understand the participants with reference to their ideals and personal experience (Winberg, 1997:112). Another reason why the researcher decided to use a qualitative research is because it includes data gathering techniques such as interviews and case studies which assisted the researcher to get to the real answers because it is based on experience (Pope, Lovell & Brandl, 2001:369).

### 1.7 Population and Sampling Procedures

Salkind (1997:96) states that a population is a group of potential participants to whom you want to generalise the results of a study. Wellman and Kruger (1999:46) states that a population is the study of objects which may be individuals, groups, organisations, human products and events or the conditions to which they are exposed. The ideal population for this research will be all investigators involved in the investigation of credit card fraud. This is however impossible because it will cost a lot of money and take up a lot of time. The researcher therefore decided to use a study population. A study population is the aggregation of elements from which the sample is actually selected (Maxfield & Babbie, 1995:186). The study population in terms of this study is members from the three Commercial branches of the SAPS in the Gauteng Province, forensic investigators employed in the four major banking institutions in the Johannesburg and Pretoria area investigating credit card fraud, and Risk managers employed at Nami-Tech, the manufacturing company of credit cards in South Africa. The target population comprised 140 investigators from the SAPS, 55 investigators employed by the banks and five Risk managers employed at Nami-Tech. This gave the researcher a total of 200 investigators in terms of the target population. The researcher decided to select a sample of 30 from the study population. A sample is the selection of members from a population and is used to make statements about the whole population (Blaickie, 2003:16). The researcher regarded the sample to be representative of the population because they all deal with credit card fraud on a daily basis and are specialist investigators who administer the same laws. They can therefore be considered to represent all

investigators. Each investigator also has five years or more experience in the investigation of card fraud.

The researcher decided to use random sampling as a selection method because in random selection each element has equal chance of selection independent of any other event in the selection process (Maxfield & Babbie, 1995:221). To select the sample from the study population the researcher used the simple random sampling technique. Simple random sampling involves a selection process that gives every possible sample the same chance of selection. Each element of a population must be able to be identified and numbered. The selected numbers then determine which population elements are to be included in the sample (Blaickie, 2003:168). An alphabetic name list was requested from the different Commercial branches in the SAPS, banks and Nami-Tech. Each Commercial Branch member's name was written on pieces of paper folded and placed in a hat. The researcher then randomly drew a total of 16 names from the hat. The same process was used for the selection of risk managers from Nami-Tech and a total of two names were drawn from the hat. The banks which included First National Bank, ABSA, Nedbank and Standard Bank were all drawn independently from each other. Names of investigators employed at ABSA bank were the first to be placed in the hat and a total of three names were randomly selected. The same process was applied to the remaining banks giving the researcher a total of 12 names. For the sample a total of 16 investigators were chosen from the SAPS, 12 from the banks and two risk managers from Nami-Tech.

### 1.8 Data Collection

The following qualitative data collection techniques were used:

#### 1.8.1 Literature

The researcher made use of national and international sources in the area of policing, law, investigation of crime, criminology and sources from the Internet. Identified sources were consulted in order to obtain relevant information which

covered the topic's aim and research questions. There is, however, no literature available with the same topic as this research. There are a number of reports on the unique security features of credit cards in the United Kingdom, Australia and the United States of America which the researcher consulted and made use of. Locally there has also been some research on the unique security features of a credit card in general by banks and the Fraud Research Centre at University of Johannesburg. There is also a fraud website in South Africa: www.whitecollarcrime.co.za.
http://www.whitecollarcrime.co.za/tips/creditcard.htm (31 March 2005), which the researcher has consulted and from which information was used.

Due to the fact that there is no literature available with the same topic as the research and to find more and relevant material it was decided that the topic be divided into different sections which were identified in order to find literature, namely:

- Identification
- Forensic investigation
- Locard Principle
- Credit cards
- Credit card fraud

Any literature found was studied and information that addressed the research questions and aims of this study were identified and selected for use. The researcher made use of different card figures issued by VISA International in the discussion, the researcher however did not get permission from VISA International to use the card templates. The personal particulars endorsed on the cards are imaginary and not real.

### 1.8.2 Interviews

Arksey and Knight (1999:2) state that interviewing is a process that provides data on understandings, opinions, what people remember doing, feelings and the like

that people have in common. Interviews may be more exploratory and qualitative, concentrating on the distinctive features of situations and events and upon the beliefs of individuals or sub-cultures. The reason for using interviews is that it can yield a great deal of information because people with experience are interviewed.

For the purpose of this study structured and focus group interviews were used.

#### 1.8.2.1.1 Structured Interviews

In a structured interview, the interviewer poses a collection of questions from a previously compiled schedule, known as an interview schedule, to a respondent and records the latter's response (Wellman & Kruger, 1999:160). The interviews were conducted face to face and the interview schedule comprised open-ended questions relevant to the research question. The reason for the use of open-ended questions was that it allowed the respondents to answer more fully on questions posed. Because the interview was based on a qualitative study which resulted in a more flexible interview and which yielded more information which the researcher did not plan for. The questions were structured in such a way that it addressed the research question and the researcher ensured reliability and validity by recording the interview.

The researcher followed the guidelines given by Leedy and Ormrod (2005:159) for conducting a productive interview:

- Make sure your interviewees are representative of the group.

  The researcher interviewed respondents who are credit card investigators and involved in the manufacturing of credit cards. These respondents were therefore expected to provide typical perceptions and perspectives on the security features of a credit card.

- Find a suitable location.

  All interviews were conducted in offices with lock and key. This ensured that there were no interruptions and distractions and the place was quite and peaceful.

- Take a few minutes to establish rapport.

  During the interviews the researcher always started by building rapport, asking the respondents about their families, discussing gardening, sport, etc. The researcher ensured that he was courteous and respectful at all times.

- Get written permission.

  The researcher ensured that written permission was obtained in advance by forwarding consent forms to all respondents asking them to sign and agree to an interview. All respondents agreed to the interview and confirmation was received upon receipt of the consent forms from respondents. The researcher did not attach the original consent forms to the dissertation because of confidentiality reasons, but will keep the form for a period of three years after the degree is approved.

- Focus on the actual rather than on the abstract or hypothetical.

  The researcher ensured that he asked questions on the security features on a credit card and wanted to know how these features could be altered. The researcher did not place emphasis on asking questions on policies and procedures, etc.

- Don’t put words in people’s mouth.

  At no stage during the interviews did the researcher suggest or try and change the manner in which the questions were answered. The actual words spoken by the respondents in response to questions were recorded.

- Record response verbatim.

  All interviews were recorded. The researcher ensured that answers to all questions were captured on tape exactly as was stated by the respondents. Permission was obtained from respondents to use the tape and the recorded interview.

- Keep your reactions to yourself.

  The researcher ensured that he was listening attentively and did not at any stage show expressions of surprise or disapproval when listening to the respondents.

- Remember that you are not necessarily getting the facts.

  The researcher was aware that the interviews were not going to reveal factual information only.

- Confidentiality.

  The researcher ensured that the identity of respondents was kept confidential and therefore the use of the term respondents was used in the research rather than stating their names.

#### 1.8.2.2 Focus Group Interviews

The research started with focus group interviews. The purpose of having a focus group is to test the interview schedule. After the focus group interview the researcher adjusted the interview schedule to address the weak points. A focus group is a special type of group in terms of size, purpose, composition and procedures. The purpose is to listen and gather information and it is a way to better understand how people feel or think about an issue, product or service (Moustakas, 1990:41). The researcher invited a total of 10 participants from the SAPS, the banks and Nami-Tech (card manufacturing company) to discuss the unique security features on a credit card with the aim of identifying possible fraudulent use. The ten participants were selected by using the simple random sampling method as described by Blaickie (2003:168) and which included the respondents from the sample. All the names of the SAPS investigators were placed in a hat and four names drawn. The same procedure was applied to both the bank investigators and risk managers from Nami-Tech. Four investigators from the SAPS commercial branch, four investigators from the banks and two risk managers from the manufactures of credit cards were selected and invited to discuss and participate in this study. Leedy and Ormrod (2005:159) state that focus groups are especially useful when time is limited. They also point out that people sometimes feel more comfortable talking in a group rather than alone and that interaction amongst participants may be more informative than individually conducted interviews and when the researcher is having difficulty interpreting what was observed. The researcher used this method and was able to obtain

perceptions from the respondents on the defined area of interest in a permissive non-threatening environment due to the fact that the discussions were relaxed and often the participants enjoyed sharing their ideas and perceptions. This was also an ideal situation for the researcher to test the interview schedule in order to determine whether the questions provided the expected results. The response to the questions and the answers provided by the participants provided the researcher with positive results and was in line with what the researcher expected. The interviews were recorded on audiocassette and transcribed later. The transcription was then analysed and the information categorised thematically.

#### 1.8.2.3 Case Studies

Leedy and Ormrod (2005:114) states that a case study is a type of qualitative research in which in-depth data is gathered relative to a single individual, programme or event, for the purpose of learning more about an unknown or poorly understood situation. The researcher collected extensive data on card fraud. The cases included police and bank case dockets. Docket analysis was employed on the withdrawn and closed dockets in order to examine the case dockets and identify the unique security features that have been altered. The researcher obtained a total of 100 fraud police dockets for the period 2005/05/01 to 2005/12/01 on credit cards from the Sandton police station. Verbal permission was obtained by the researcher from the detective branch commander at Sandton SAPS to read the case dockets and use the data in the dockets for research purposes. Using the systematic sampling method as described by (Leedy & Ormrod, 2005:202) the researcher obtained a sample of 38 withdrawn and closed police dockets and 12 bank case docket giving the researcher a total of 50 case dockets. The case number of each police docket was recorded on a separate piece of paper, folded and placed into a hat. A number comprising of both even and odd numbers from one to hundred were recorded on the front of each of the folded pages. The researcher tossed a coin. Heads determines that we begin drawing even numbers from the hat and tails determine the drawing of odd numbers. The coin was tossed and came down heads. This meant that the researcher started with

the first even number which is two and selected systematically sequential numbers four, eight, 10, 12,14,16 etc, until a total of 38 dockets was obtained. The same principle was applied to the bank case dockets. They were however drawn independently. The researcher started with First National Bank and placed six case numbers in a hat allocated with odd and even numbers up to the number six, three case numbers were drawn. The same procedure was employed for the three remaining banks giving the researcher a total of 12 case dockets. This provided the researcher with a total of 50 case dockets.

Dockets were studied to:

- Identify the security features that were fraudulent.
- Identify which security feature was most commonly altered.
- Identify the different security features endorsed on a credit card. This was achieved by inspecting the exhibit (credit card) filed in the case docket.
- Identify the difference between a genuine and altered security feature. This was achieved by inspecting the fraudulent card security features in the case docket compared with a genuine credit card.

### 1.9 Data Analysis

Leedy and Ormrod (2005:152) states that data analysis involves the categorisation of data according to its meaning and in which patterns, regularities and critical events are identified. The researcher transcribed interviews to facilitate the collection of information. Leedy and Ormrod (2005:153) provide a framework to be followed after the transcribing of interviews which the researcher followed:

- Identify statements that relate to the topic

The researcher did this in order to separate the relevant from the irrelevant information in the interview and then broke the relevant information into small segments/sentences which reflected a single specific thought.

- Group statements into meaningful units

The researcher did this by ensuring that the sentences were grouped into categories that reflect the various meanings of the phenomenon as is experienced.

- Seek divergent perspectives

The researcher did this by considering the various ways in which the respondent provided answers in the interviews.

- Construct a Composite

The researcher identified the various meanings and developed an overall description of the research topic that is in question.

Case studies were analysed by using the grounded theory study. Leedy and Ormrod (2005:154) state that grounded theory studies use a prescribed set of procedures for analysing data and constructing a theoretical model from them. In this study the researcher used the coding procedure whereby data from the case dockets were scrutinised for commonalities and where then categorised into themes. The researcher, after the categorisation of the data, further examined the data for specific attributes that distinguished and characterised the security features of the credit card. By using this procedure the researcher was able to reduce the data into smaller sets of themes to identify and describe the unique security features of the credit card. Where possible, all information from the interviews were coded and combined with docket analysis information.

### 1.10 Validity

According to Neumann (2000:165) “validity” addresses the questions of how well the social reality being measured through research matches with the constructs that researchers use to understand it. Validity concerns the accuracy of the questions asked, the data collected and the explanation offered. Generally it relates to the data and the analysis used in the research (Denscombe, 2002:100). The researcher ensured that the above points where adhered to by firstly testing the interview schedules during the focus group interviews before the researcher proceeded further. The researcher ensured that the data collected was valid because all the books, journals, periodicals and internet information consulted were relevant to the topic. The interviews were valid because the researcher interviewed investigators who worked in the field of credit card fraud.

## 1.11 Reliability

Neumann (2000:165) explains reliability to mean dependability or consistency. Reliability relates to the methods of data collected and the concerns that they should be consistent and not distort the findings. Generally it entails an evaluation of the methods and techniques used to collect the data (Denscombe, 2002:100). The researcher ensured that the above was adhered to by applying the same testing instruments, namely interview schedules and docket analysis pro-forma, to all interviews and dockets analysed. From the interviews conducted and the data collected the researcher obtained the same type of responses which resulted in saturation levels being achieved which was one of the testing instruments the researcher used to ensure reliability. The data collected were from books, periodicals, journals and the internet which were all relevant to the topic. The researchers interviews were reliable because all respondents interviewed worked with credit card investigations and manufacturing. The researcher ensured that the analysis was valid because he used the approved data analysis spiral which is tested and included the synthesis, classification, perusal and organization of data as explained by Leedy and Ormrod (2005:161).

## 1.12 Ethical Considerations

Ethical consideration in the research was addressed by adhering to the Code of Ethics for Research of Unisa (Unisa, policies and procedures for postgraduate studies, 2002:26). Adhering to this research code, the researcher ensured that all sources used, including information obtained from the case dockets, was properly referenced and all sources of information were acknowledged. Ethical consideration was further adhered to as explained by (Leedy & Ormrod, 2005:107):

- Request permission from the relevant authorities and businesses to undertake the research.

  The researcher obtained prior permission from the SAPS (permission attached) and Nami-Tech to conduct the research. Permission was further

obtained from each respondent but due to confidentiality the researcher did not include it in the dissertation. The researcher will however keep this information for a period of three years.

- Ensure that all the participants agree voluntarily to be interviewed by obtaining their consent.

  The researcher obtained the consent from all respondents by forwarding an acknowledgement of consent form which required the signature of all respondents who were willing to be interviewed.

- Ensure the anonymity of the participants and protect their identity.

  The researcher ensured that all participants' details were treated with the strictest of confidentiality and privacy and did not make any of these details available to any person. All information was kept under lock and key in a study cabinet at the researcher's place of residence. The researcher further scanned and stored the information electronically which is kept in a safe under lock and key at the researchers place of residence.

- Ensure that the correct sampling techniques are used.

  The researcher ensured that all respondents who participated in the research were individuals who investigated credit card fraud and worked in the credit card industry and who could be considered specialists in this field.

- Maintain the standards by engaging proper referencing techniques and acknowledging all sources of information.

  The researcher ensured that there was no fabrication, forging and falsification of data or plagiarism and that all sources were acknowledged by engaging in proper referencing methods.

### 1.13 Chapter Outlay

The report is divided into the following chapters.

- Chapter two: Credit Card Fraud

  In this chapter the researcher explains the concept of credit card fraud and also discusses the difference between forensic investigation and forensic

science. The researcher further explains the elements of fraud and the different types of credit card fraud.

- Chapter three: Unique Security Features.

  In this chapter the researcher identifies and explains the unique security features found on a credit card

- Chapter four: Preventative Counter-measures

  The researcher discusses the various countermeasures put in place to prevent fraudulent manipulation.

- Chapter five: Findings and Recommendations

  The researcher listed findings and recommendations formulated from the research conducted.

# CHAPTER TWO
# CREDIT CARD FRAUD

## 2.1 Introduction

The bank card industry originally developed in the United States of America and traces its roots back to 1914 when Western Union issued the first consumer charge card. The use of credit cards has become a way of life in many parts of the world. The enormous growth of credit cards has left many law enforcement agencies with mixed emotions. All credit cards have one thing in common, namely that the bearer can obtain something of value simply by presenting the card (Visa International Law Enforcement Education Programme, 2004:29). The card, therefore, is valuable and should be provided with reasonable protection by the cardholder. Credit card issuers have explored a variety of security alternatives over the years. Visa International constantly reviews security measures that may be applied to cards and devotes considerable resources to maintenance of security systems and programme. These programmes mandated by the association include uniform card standards, security standards for the manufacturer, embossing and encoding of cards. The association's goals of constantly reviewing security methods are to create a card that is technically difficult to alter or counterfeit.

The credit card is unique in that the utilization history can be obtained through the card issuer's records. Today, credit cards are used like currency. They are used for travel, car rental, lodgings, food and any other service where cash would be a requirement (Visa International, Law Enforcement Education Programme, 2004:113). No security system is perfect, especially not one that passes through millions of hands, as do credit cards. Security measures are becoming rigorous. Credit cards today are much harder to forge than before, and new security procedures make it harder to misuse a lost or stolen card. The SAPS Detective Training Manual (2004:86) state that "the principle duty of the police when an offence is reported to them is to trace the alleged offender, bring him before the court and produce all available evidence. In order to achieve this object the facts

of a case must be ascertained inter-alia through questioning the complainant, informant and any witnesses. When this has been done a separate detailed statement must be taken from each person interrogated, giving, in the order of occurrence, all the facts to which he is prepared to testify".

The discussion to follow will concentrate on forensic investigation and the differences that exist between forensic investigation and forensic science as well as a comprehensive discussion on fraud and the elements of the crime fraud.

## 2.2 Forensic Investigation

According to Davia (2000:121) forensic investigation is divided into two concepts, namely, forensic science and forensic investigation. Slyter (1995:21) explains that forensic investigation is a process of collecting facts that can serve as evidence before a court of law, through which the associative part of an accused in the commission of the crime can be proved. When asked the question, "what is forensic investigation?", five respondents stated that forensic investigation involves the use of scientific methods and techniques in order to reconstruct the circumstances of the act of omission. Fifteen respondents stated that forensic investigation is another term for criminal investigation, whilst 10 respondents stated that forensic investigation is a process of compiling a criminal file and forwarding to a court for prosecution.

The viewpoints as expressed by the respondents differ to an extent and the reason can be attributed to the fact that the term "forensic investigation" in the past has always been associated with investigations conducted by experts in a laboratory. Grabosky and Smith (1998:151) state that forensic investigation is all about detecting the truth and the truth means nothing if it is not supported by evidence. It is a process during which the witnesses, exhibits (for example, in the form of documentary proof) and suspected offenders are identified.

Today it is a common fact that traditional police investigative resources no longer are equipped to handle the growing complexities of crimes such as fraud, theft and corruption. This has given rise to what is now referred to as a "forensic investigation", whereby the private sector has created multi-disciplinary investigation teams incorporating such disciplines as information technology, accountancy and law which work together with the police in one investigation team (Rose, 1995:201).

Gup (1995:12) states that when a decision is to be made on who will be the most appropriate to conduct a forensic investigation, the following potential options based on the Constitution of South Africa, as well as legal entities within the framework of South African law, should be considered;

### 2.2.1 The Police

In terms of section 205 (3) of the Constitution of the Republic of South Africa, Act No. 108 of 1996, the powers and functions of the South African Police Services (SAPS) is the investigation of any offence or alleged offence. In terms of the South African Police Service Act, 1995 (Act No 68 of 1995) the SAPS is responsible for the investigation of all crimes committed. It is therefore the duty of every member of the SAPS to investigate crime as effectively as possible. The crime investigating official has a greater responsibility in the investigation of crime and therefore has to investigate cases with greater effectiveness and professionalism. Further the investigator has to trace the criminal, gather the necessary evidence regarding the crime and to take the case to court (South African Police Service, Detective Training Manual, 2004:1).

With reference to a forensic investigation, a SAPS investigator must obtain classified information from banking institutions, for example, bank statements and all bank account information, statements and documentary proof in dispute or under investigation. On receipt of this information a forensic report must be compiled by the investigator. Forensic investigation requires that the police are

involved from the initial phase up until the presentation of a case to court, the reason being that the Criminal Procedure Act stipulates that only the police can bring a case before a criminal court (Sorgdrager & Oudkerk, 1997:1).

### 2.2.2 Contract External Auditors

The Auditing Profession Act No. 26 of 2005 (Act No. 1 of 2005) provides for the investigation into or review of any unlawful act or omission committed by any person responsible for the management of an entity which:

- has caused or is likely to cause material financial loss to the entity or to any partner, member, shareholder, creditor or investor of the entity in respect of his, her or its dealings with that entity; or
- is fraudulent or amounts to theft; or
- represents a material breech of any fiduciary duty owed by such person to the entity or any partner, member, shareholder, creditor or investor of the entity under any law applying to the entity or the conduct or management thereof.

Auditors are used at the initial phase of an investigation and are generally responsible for verifying financial reports, analysing specific records and information. They also look out for irregularities, fraudulent activities, maladministration and corruption when inspecting financial journals and books, which can lead to a forensic investigation being conducted. Auditors are used to give evidence as expert witnesses in courts.

### 2.2.3 Corporate Investigators

The Private Security Industry Regulation (PSIRA) Act No. 56 of 2001 [Section 2(1) (f)] authorises corporate investigators to:

- conduct normal and reasonable investigations into misconduct by employees, and;

- conduct investigations which a business may undertake in the course and scope of its normal and reasonable endeavours to safeguard its security, strategic, operational or business interests.

These investigators are used at the initial phase of an investigation and are responsible for obtaining statements, documentary evidence and they can serve as witnesses. They are appointed by companies to investigate irregularities within such companies, to identify crimes within the organisations and to prepare preliminary investigations and forward the same to the police for finalisation and presentation to court.

### 2.2.4 The National Prosecution Authority

Section 179 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) created a single National Prosecuting Authority (NPA). The National Prosecuting authority has the power to:

- institute and conduct criminal proceedings on behalf of the state;
- carry out any necessary functions incidental to instituting and conducting such criminal proceedings including investigations; and
- discontinue criminal proceedings.

On 25 June 1999 the President committed the government to the establishment of a crime fighting capacity to effectively investigate and prosecute priority crimes in South Africa. On 8 July 1999 the Minister of Justice and Constitutional Development on behalf of the President of South Africa, announced the establishment of the Directorate of Special Operations (DSO). The launch of the DSO on 1 September 1999 was a powerful step towards putting in place the necessary machinery to eradicate organised crime in South Africa.

The Office for Serious Economic Offences, established in 1992 in terms of the Investigation of Serious Economic Offences Act (No 117 of 1991), was incorporated into the National Prosecuting Authority as an Investigating

Directorate in terms of Section 43 (7) of the Act. The Investigating Directorate: Organised Crime and Public Safety was established by Presidential Proclamation R102 of 1998 published in the Government Gazette No 19372 on 16 October 1998 was also incorporated into the National Prosecution Authority as an Investigating Directorate in terms of Section 43 (7) of the Act. A further Investigating Directorate: Corruption was established in terms of Proclamation R14/2000, published in the Government Gazette No 20997 on 24 March 2000.

The Directorate of Special Operations, although transitionally operational under the auspices of the above-mentioned Investigating Directorate, was only legally created in terms of the Act which came into operation on 12 January 2001 of R3/2001, published in the Government Gazette No 21976 on 12 January 2001.

### 2.2.5 Special Investigating Unit

The Special Investigating Unit and Special Tribunal Act No. 74 of 1996 provides for the investigation into serious malpractices or maladministration in connection with the administration of state institutions; state assets; public money and any conduct which may seriously harm the interest of the public.

The functions of the special investigating unit include:

- investigating all allegations brought to the attention of the unit;
- collecting evidence regarding acts or omissions which are relevant to its investigation and, if applicable, to institute proceedings in a special tribunal against the parties concerned;
- presenting evidence in proceedings brought before a special tribunal; and
- referring evidence regarding or which points to the commission of an offence to the relevant prosecuting authority.

## 2.3 Forensic Science

Forensic science is a study of the nature and behaviour of natural things with regulations to the law (Slyter, 1995:28). Forensic science involves the search for

and examination of physical clues within the confines of a laboratory that might be useful in establishing or excluding an association between someone committing a crime and the scene of the crime or victim. Such traces of physical clues include, for example, body fluids, hair, textile fibers from clothing. Forensic science can simply be defined as the application of science to the law (Davia, 2000:121). The field of forensic science has grown tremendously, leading to a considerable expansion in forensic laboratories, both in size and scope of operations. The application of forensic science in criminal investigation has rapidly expanded with the recognition that physical evidence occurs in many useful forms. Forensic science is therefore an important aid in forensic investigation (Lee, 2000:17).

Rapp (1991:54) explains that credit cards are made with polyvinyl chloride plastic (PVC) and therefore, examination of the counterfeit plastic composition by a forensic chemist can be useful in specific cases. Analysis of various cards and known samples can determine the source of the plastic and whether the cards in question have a similar composition. Additionally, forensic examination of a cards printing, embossing and inks can also be useful in determining the relationship between counterfeit cards in question.

## 2.4 Fraud

The crime of fraud has a long history and the first widely known commission thereof can be found in the holy Bible. Jacob and his mother intentionally mislead his father, Isaac, so that Jacob could be blessed instead of Esau. Esau was intentionally prejudiced because of this misrepresentation. He was denied of his birthright and Jacob obtained certain rights, which he would not have been entitled to otherwise (South African Police Service, Basic Fraud Course, 2000:1).

Fraud is derived from the Latin word falsum, which means falsification (South African Police Service Advance Training Manual Commercial Crime, 2002:78). Initially, actual prejudice was required, but over the years the circumstances and

requirements of fraud have been amended so that potential prejudice is now sufficient to constitute the crime of fraud (Corner, 2003:23). Fraud is a crime that can be committed in various ways. The current technological development of, amongst others, computers and credit cards lends itself to exploitation by criminal elements that are usually from the upper levels of society. Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another (Snyman, 2002:504).

On the question relating to the definition of fraud, all respondents were knowledgeable with the definition of fraud. This merely highlights the researcher's point that all the respondents are suitable for participating in this research and that they are specialist in their field of investigation.

### 2.4.1 Elements of Fraud

The elements of fraud are misrepresentation (or distortion of the truth), unlawfulness, intention and prejudice (Snyman, 2002:505).

#### 2.4.1.1 Misrepresentation (Act)

One of the elements of all crimes is an act. This consist of voluntary human conduct which can manifest itself in either the doing of something (commission) or the failure to do something which the law requires to be done (omission) (South African Police Service, Basic Fraud Course, 2000:06).

The very first requirement for fraud is that there should be a misrepresentation or, as it is sometimes expressed a "perversion or distortion of the truth" (Snyman, 2002:505). Misrepresentation is defined as the distortion of the truth which can be made verbally, in writing, expressly or tacitly (Snyman, 2002:505). An individual must represent to another individual that a fact or a set of facts exists which in truth does not exist. Snyman (2002:505) defines misrepresentation as a perversion or distortion of the truth. Misrepresentation usually takes the form of spoken or written words, but it may also take the form of conduct by means of nodding

one's head. In this regard, South African Police Service, Advance Training Manual, Commercial Crime (2002:81) states that this is not sufficient to constitute fraud and in order to be classified as fraud, a misrepresentation must also have a bearing on the other elements of the crime. These are that:

- It must be an untrue fact.
- The presenter must know that it is untrue or be indifferent as to its truth.
- It must have been intended or calculated to induce the victim to act upon it.
- The person to whom it is made or someone else must suffer actual or potential prejudice as a result thereof

Here is an example: X has in his possession a forged credit card but he does not present it to any person. The misrepresentation is thus incomplete and X does not commit the crime of fraud.

#### 2.4.1.1.1 Forms of Misrepresentation

A misrepresentation can be made in different ways, namely: in writing, verbally, a combination of words and conduct (commission), by silence (omission) or by expressing a belief that is not in fact held (South African Police Service, Advance Training Manual, Commercial Crime, 2002:126).

#### 2.4.1.1.1(i) Misrepresentation by words

This is the most common way in which a misrepresentation is made and usually amounts to the telling of a lie for the purpose of inducing someone else to believe that it is the truth (South African Police Service, Basic Fraud Course, 2000:10). For example, a breeder of stud horses sells a stallion to a buyer. He is aware that the stallion is not pedigree but represents to the buyer in words that it is. In the case of S v Shaban 1965 4 SA (W) the court ruled that when minutes are taken at a director's meeting, the omission of certain words in the minutes of that meeting constitutes a misrepresentation.

**2.4.1.1.1(ii) Misrepresentation by conduct**

A misrepresentation can be made through conduct alone. According to South African Police Service, Advance training Manual, Commercial Crime (2002:91), a representation needs not be made in express words; it may be made by conduct. In the case of (R v Larkins 1934 AD 91) the accused induced the complainant to give him a cheque (as a loan) by representing to him that he would repay him out of his salary at the end of the month. The accused had, prior to that, ceded the full amount of his salary to someone else. The court held that a representation need not be made in express words, but in conduct alone. His conduct comprised of his silently pretending to the complainant that he had full title to his salary whilst in fact he had already ceded such title.

**2.4.1.1.1(iii) Misrepresentation by failure to disclose**

A misrepresentation can also be made by omission, that is, by failure to disclose a material fact to the other party, which, unless revealed, can induce the other party to act to his own or another's prejudice (South African Police Service, Detective Training Manual, 2004:5).

South African Police Service, Advance Training Manual, Commercial Crime (2002:108) states that the requirements of an omission include, a duty to disclose the particular fact:

- a wilful breech of this duty under such circumstances as to equate the non-disclosure with a representation of the non-existence of the fact; and
- an intention to defraud, which, as Gup (1990:85) points out involves the following:
    - knowledge of the particular fact;
    - awareness and appreciation of the existence of the duty to disclose; and
    - deliberate refraining from disclosure in order to deceive and induce the representee to act to its prejudice or potential prejudice.

## 2.5 Unlawfulness

Grabosky and Smith (1998:132) explain that the unlawfulness in fraud consists in the making of a misrepresentation with the intent to cause prejudice. Grounds of justification, such as consent and acting on an order, may exclude the unlawfulness of the act. Unlawfulness is an objective element of a crime and the unlawfulness of an act is ascertained without reference to the perpetrators state of mind (Grabosky & Smith, 1998:134). Where a particular act or omission has not previously been identified as being unlawful the courts takes it upon themselves to determine the matter. Snyman (2002:145) states that the general rule is that the unlawfulness of an act or omission is determined according to the perception of society as to what is legally "wrong or right", at any given time. It must be proved that the accused was wrong and, to prove his intention, that he knew that it was wrong. It must also be proven that no grounds of justification existed at the time of the act.

## 2.6 Intention

Fraud can only be committed intentionally. Fraud cannot be committed negligently. Fischer (1999:131) explains that a person has intention if the person:

- Makes a misrepresentation intentionally;
- Knows that it is going to mislead another;
- Knows that it is unlawful;
- Knows that prejudice or potential prejudice can arise from the misrepresentation.

South African Police Service, Basic Fraud Course (2000:13) states that the perpetrator must have the intention to both deceive, that is, the intention to induce another to believe that something is true which, in fact, is untrue, and to defraud, that is, the intention to induce somebody to act to his prejudice on the grounds of the misrepresentation. For example, X presents a credit card in which the security

features have been altered. X knowingly and intentionally misleads the person receiving the card that the card is genuine and it is good for the transaction.

## 2.7 Prejudice

In many instances in fraud the person to whom the misrepresentation is made is in fact prejudiced. Fischer (1999:142) explains that prejudice is to decide beforehand or to lean in favour of one side of a cause for some reason or other than it's justice. The prejudice can either be actual or of a potential nature. Snyman (2002:507) states that the "risk of the prejudice need not be probable, direct or reasonably certain; all that is required is a reasonable possibility of prejudice". Actual prejudice requires that the distortion of the truth must lead to another suffering actual prejudice. For example, X is a businessman and pretends to be a director of a company. He tells B, that B, should buy shares from his company. The share certificates are forged. B has no idea that X is tricking him and pays a sum of money for the forged share certificates. X, committed fraud. The misrepresentation of X caused B, to suffer an actual prejudice.

### 2.7.1 Potential Prejudice

If a misrepresentation is potentially prejudicial to another, this still constitutes fraud. Therefore there need not be actual prejudice (Snyman, 2002:507). In (R versus Heyne 1956 3 SA 604 A) A and B were owners of a bottle store. They neglected to keep proper records of their sales and also made some false entries into the books. They were found guilty of fraud because through their conduct they made false representations to the police and which would at least potentially prejudice the state.

The prejudice or potential prejudice need not necessarily be proprietary. In State versus JASS (1965 3 SA 248 OK), A showed a forged drivers license when he was asked to present it in court. The question is whether his misrepresentation has any actual or potential proprietary prejudice to anyone. The court ruled that the prejudice need not be proprietary.

## 2.8 Types of Credit Card Fraud

Credit card fraud has taken many forms, from thieves using stolen credit or debit cards to buy goods to the greater, more sophisticated problem of criminals altering security features. Despite a host of hi-tech anti–fraud measures, the battle against fraud continues as criminals continue to poke and prod at the card industries weak spots (Visa International, 2002:8). Credit card fraudsters are an ingenious group of people. Over the past 30 years criminals have been able to side step nearly every fraud prevention measure developed by the card industry (Gup, 1995:123). In the early days of the card industry, card fraud was a crime of opportunity, originating from a sales slip found in a dustbin or a card found in a lost or stolen wallet. Today's criminals are nearly as technologically advanced as the card industry, as quickly as the card industry introduces high-tech fraud prevention measures, criminals just as rapidly find ways to breach them (Rapp, 1991:18). The crime of fraud itself has evolved into a highly organised business that reaches around the world.

With the widespread use of credit cards, credit card fraud has become an easy source of income for criminals. Criminals perpetrate credit card fraud by presenting lost or stolen credit cards and counterfeit credit cards. According to the recent statistics released by South African Banking Risk Information Centre (SABRIC) for the year 2006/01/15 to 2007/01/15 with reference to credit card fraud, there is a 78 per cent increase in this type of crime nationally in South Africa. Statistics compiled by the Provincial Office of the SAPS, Commercial Crime Branch, Gauteng for the period 2006/01/15 to 2007/01/15 indicates an 80 per cent increase in credit card fraud (Annual Statistics, SAPS Commercial Branch, Gauteng, 2007:10).

There are different types of credit card fraud ranging from counterfeit card fraud to lost and stolen card fraud. Lost and stolen card fraud is more of an opportunistic fraud type and can be controlled by precautionary measures being

adopted by cardholders, whilst counterfeit card fraud involves a number of technological fraud types such as skimming, cloned cards, altering of information on the magnetic stripe and the re-embossing of details onto cards (Rapp, 1991:23).

### 2.8.1 Fraud with Stolen and Lost Credit Card

This category of fraud occurs on cards which have been reported by the cardholder as lost or stolen. Most fraud in this category takes place in shops before the cardholder has reported the loss (Rapp, 1991:12). Fraud with stolen and lost credit cards is the most common type of credit card fraud and involves the theft of genuine card details that are used to make a purchase through a remote channel such as the phone, fax, mail order or the Internet. As with counterfeit cards fraud, the legitimate card holder may not be aware of this fraud until they check their bank statements. Statistics released by the South African Banking Risk Information Centre (SABRIC) for the period 2006/01/01 to 2006/12/01 on lost and stolen cards amounted to R22 million. The problem in countering this type of fraud lies in the fact that neither the card nor the card holder needs to be present at the point of sale. This means that:

- The merchants are unable to check the physical security features of the card to determine if it's genuine.
- Without a signature or a pin it is not easy to confirm the customer is the genuine card holder.
- Card issuers cannot guarantee that the information provided in a card not present environment relates to the genuine card holder.

An example from the case Law could be found in (S v SALCEDO 2003 (1) SACR 324 SCA) where the accused committed credit card fraud by picking up a credit card in a mall which had fallen out of the account holders pocket and going on a spending spree on the same day. The accused was convicted on nine counts of fraud and sentenced to six months imprisonment on each count.

With regard to the question concerning what initiatives are in place to address lost and stolen card fraud, 12 respondents indicated that the banking industry has a retail education programme which provides help for shop staff on how to detect stolen cards at the point of sale. Fourteen respondents indicated that an industry hot card file enables retailers to electronically check whether a card has been reported lost or stolen, whilst four respondents indicated that the banking industry has computer systems in place to track customer accounts and detect unusual spending patterns.

### 2.8.2 Counterfeit Card Fraud

A counterfeit or skimmed card is one that has been printed, embossed or encoded without permission from the issuer or one that has been validly issued and then altered or recoded (Gup, 1995:133). A counterfeit card is one that is illegally manufactured. It is embossed and may have the magnetic stripe encoded with the appropriate information from a legitimate card which had been electronically compromised. Visa International Law Enforcement Education Programme (2000:125) describes a counterfeit card as a genuine credit card manufactured by a certified printer but which has one or more features changed by mechanical or electronic means. Most cases of counterfeit fraud involves skimming, a process where the genuine data on a cards magnetic stripe is electronically copied onto another, without the legitimate cardholder's knowledge http/www.cardwatch.org.uk/html/skimming_info.html (31 March 2005). South African Police Service, Advance Training Manual, Commercial Crime (2002:126) states that skimming normally occurs at retail outlets, particularly at bars, restaurants and petrol stations, were a corrupt employee skims a customers card before handing it back. Often cardholders are unaware of the fraud until they receive their bank statements.

In State versus Martin Ivanoff and Other, 1999 (1) SA the accused had made available a card reader to a waitress for the capturing of credit card information. The waitress stored the device in a moon bag attached to her waist and when

receiving cards as a method of payment from customers, would swipe the card through the device which would capture and store the data. The device would be collected by the accused and the information downloaded via computer. The data transferred onto counterfeit cards was then forwarded to countries abroad and in which the credit would be utilised to the maximum.

Alterations to the security features of credit cards are usually done by a number of methods which include (Visa International Law Enforcement Education Programme, 2000:32):

- Shave and Paste: This is a process which involves carefully shaving the embossed account number off the plastic with a sharp razor blade. The numbers can then be rearranged to match a good account number and the card can be presented for purchases.
- Punching: This a process that requires the criminal to use a paper hole punch in order to punch each number out from the plastic card. By carefully placing the holes in the plastic to match a good account number the card can then be imprinted on a sales draft.
- Re-embossing: This process includes the superimposing of a good account number on a stolen or lost card. Once the card is flattened the good account number can then be embossed over the flattened number and presented for payment.

## 2.9 Credit

Credit is defined as an arrangement by trusting a person to pay for something at a later stage (Concise Oxford School Dictionary, 2002:152). Credit as a financial term, used in such terms as credit card, refers to the granting of a loan and the creation of debt. Any movement of financial capital is normally quite dependent on credit, which in turn is dependent on the reputation or creditworthiness of the entity which takes responsibility for the funds. In commercial trade, credit is used to refer to the approval for delayed payments for goods purchased. Companies frequently offer credit to their customers as part of the terms of a purchase

agreement. Credit is denominated by a unit of account. Unlike money, credit itself cannot act as a unit of account. However, many forms of credit can readily act as a medium of exchange. Credit is also traded in the market. The purest form is the "Credit Default Swap" market, which is essentially a trade market in credit insurance. Credit Finance, http://en.wikipedia.org/wiki/credit (finance) (5 December 2006).

## 2.10 Credit Cards

A credit card is defined as a financial transaction card that allows the card holder to obtain money, goods or services under a line of credit established by the card issuer (Visa International, Law enforcement Education Programme, 2004:81). Rapp (1991:120) defines a credit card as a payment card enabling holders to make purchases and draw cash up to a pre-arranged credit limit. When asked the question, "what is a credit card?" 16 respondents were familiar with a credit card and furnished an explanation similar to the definition mentioned. Ten respondents stated that the function of a credit card is to replace cash in your pocket and allow the owner immediate credit, whilst four respondents furnished explanations that a credit card can be used to make purchases and that it is a means of substituting cash.

The enormous growth of credit cards has left many law enforcement agencies with mixed emotions. On one hand the police see the credit card as creating a whole new field of criminal activity that is extremely difficult to control. On the other hand many police agencies have realized that the credit card can also provide a very useful tool for detecting and apprehending criminals. Credit cards have also provided vital evidence during investigations of burglary, robbery or even murder. An investigation of credit card crimes, therefore, promises a two-fold benefit: apprehension of the fraudulent credit card user, and information or evidence relating to other crimes. In many parts of the world the use of credit cards has rapidly become a way of life. Today both the consumer and the business

community accept credit cards. Millions of these cards are issued each year by firms ranging in size from international banks to local associations of merchants.

### 2.10.1 Types of Credit Cards

Rapp (1991:127) group electronic payment systems which use plastic cards into three categories;

1. Pay later (credit cards);
2. Pay now (debit cards);
3. Pay before (stored value or smart cards which are pre-charged with value electronically and which may be recharged).

#### 2.10.1.1 Pay Later (credit cards)

This card permits holders to obtain goods and services immediately with the card issuer providing funds to the merchant from the cardholder's account, which may be held in credit or debit (Visa International, Law Enforcement Education Programme, 2004:12). Examples of these cards include cards issued by Visa and regulated by the various banking institutions and cards issued by retail stores, for example, Edgars and Markhams.

Visa International Law Enforcement Education Programme (2004:14) explains the difference between a bank credit card and a retail store credit card as follows:

- A bank credit card can be used all over the world and it replaces the actual carrying and being in possession of money (actual physical cash).
- A retail credit card can only be used in a specific retail store. For example, an Edgars card can be used at the various retail stores that fall within the EDCON group. The card however, cannot be used at a Markhams store.

#### 2.10.1.2 Pay Now (debit card)

Rapp (1991:21) states that a debit card is a payment card linked to a bank or building society account and is used to pay for goods and services by debiting the card holders account. A debit card, or deposit access card as it is commonly

known, accesses the cardholder's funds in a cheque, savings or other form of depository account (Criminal Justice and Forensic Investigation Training Manual, 2006:162). Visa International Law Enforcement Education Programme (2000:15) explains that the debit card acts like an electronic cheque. The card holder presents the card at a point of sale and the transaction is processed through the authorisation and clearing system in which the transaction is settled against funds on deposit rather than a credit line. In 1993 Visa International introduced the debit card, a deposit access card, which accesses the cardholders' funds in a cheque, savings or other form of depository account. The debit card may also replace the cardholder's automated teller machine (ATM) card, which can be used at any available ATM with the cardholders' personal identification number (Visa International Law enforcement Education Programme, 2000:118).

Asked, what the difference is between a debit card and credit card all respondents stated that a debit card is different from normal credit cards in the sense that the card can only be used to withdraw cash via an automated teller machine or at a bank teller and were a pin number is a pre-requisite. There is also a daily limit on all cash withdrawals from an ATM imposed by banks (Rapp, 1991:15). All debit cards issued to cardholders have magnetic stripes affixed to the rear. These magnetic stripe debit cards permit transactions to be conducted and bank accounts debited immediately through the use of on-line connections between the terminal being used and the bank (Visa International Law Enforcement Education Programme, 2000:12).

**2.10.1.3 Pay before Cards (stored value cards)**

These cards have value recorded on them electronically prior to the customers using them to conduct transactions. These cards are however not issued in South Africa. The basic purpose of these cards is for purchasing small items such as newspapers, bread or milk. The single purpose of this card is to avoid theft from newspaper stands and vending machines which has been highly effective in

reducing vandalism caused to such machines and the loss of cash associated with this (Grabosky & Smith, 1998:157).

## 2.11 Debit Cards

Rapp (1991:21) states that a debit card is a payment card linked to a bank or building society account and is used to pay for goods and services by debiting the card holders account. Grabosky and Smith (1998:155) explain two types of debit card terminals that are commonly used, which are:

- Automated Teller Machines (ATM): ATMs are electronic vaults, which enable users to withdraw or deposit money or obtain other banking services.
- Electronic Fund Transfer at point of sale (EFTPOS): EFTPOS transactions are carried out using the terminal connected to a merchant cash register which enables customers to pay for goods or to withdraw cash electronically via their banks computer. Transactions are carried out by either swiping the card through the speed point machine or keying in manually the account details which then communicates details of the credit or debit of the EFTPOS network to the customer's bank.

## 2.12 VISA

The term VISA was conceived by the company's founder, Dee Hock. He believed that the word was instantly recognisable in many languages in many countries, and that it also denoted universal acceptance. The abbreviated term "VISA" is a recursive backronym for Visa International Service Association. http://en.wikipedia.org/wiki/Visa_credit_card (17 July 2006). VISA, contrary to popular belief, is not a credit card company but rather an electronic payment system that, however, did evolve from a credit card company (Visa International Law Enforcement Education Programme, 2000:3). Visa is a trans-national corporation controlled by no single interest, an association owned jointly by more than 21 000 financial institutions around the world. Through its members Visa provides a global network for value exchange. It provides worldwide telecommunications, sets operating standards, and develops new products

enabling its member financial institutions to provide their customers, both cardholders and merchants, with a convenient, low cost means of consummating a high volume of transactions throughout the world (Visa International Law Enforcement Education Programme, 2000:4).

Visa International has explored a variety of security alternatives with reference to credit cards over the years. Visa International constantly reviews security measures that may be applied to cards and devotes considerable resources to the maintenance of security systems and programmes. These programme mandated by Visa include uniform card standards, security standards for the manufacturer, embossing and encoding of cards and credit background investigations of applicants. The role of Visa is to constantly review security methods and to create a card that is technically difficult to alter or counterfeit (Visa International Law Enforcement Education Programme, 2000:12).

Today, Visa is a full service consumer payment system, the largest in the world. Through a variety of products, individuals can conduct sales transactions anywhere in the world, with confidence in the system. Any of the one billion cards currently in circulation can be used to pay for goods and services at more than 20 million locations around the world or to obtain cash at more than 647 000 cash dispensers (ATMs) displaying the blue, white and gold Visa logo (Visa International Law Enforcement Education Programme, 2000:13).

### 2.12.1 Credit Cards issued by Visa International

Unlike the credit cards issued by the retailers such as clothing departments and discount outlets, which bear the store name and are good only in that store, for example an Edgars card, there is no charge for this type of card because it is a way of building up a captive clientele (Rapp: 1991:16). The credit card issued by Visa International via the various banking institutions is a much more sophisticated product which contains a number of security features.

Rapp (1991:16) states that there are two ways in which a cardholder uses a credit card:

- To obtain merchandises or services, by physically presenting a credit card at a point of sale terminal. The point of sale terminal function allows for the authorisation of a credit card. Essentially credit card authorisation permits a merchant to obtain immediate approval in order to honour a customer's credit card (Rapp, 1991:16). The transaction begins when the card holder presents his or her card to a merchant for the purchases of goods or services. Visa International Law Enforcement Education Programme (2000:16) explains that merchants are required to follow established procedures which include:
    - obtain authorisation for the sale;
    - obtain the imprint of the card, either manually or electronically; and
    - obtain the signature of the card holder and compare it to the signature on the card.
- To obtain cash from automated teller machines.

The four major banking institutions in South Africa namely, ABSA, First National Bank, Standard Bank and Nedbank are all affiliated to Visa International. They, therefore, issue Visa International cards, as well as other services provided by Visa International (SABRIC, 2004:12). All Visa cards are uniform in standard and there is no vast difference with reference to the security features found on the different types of credit cards. The most distinguishable difference is the difference in colour on the different credit cards (Visa International Law Enforcement Education Programme, 2000:2).

Almost everyone has seen credit cards and has some idea about how people use them. However, few people are aware of the exact differences between various types of credit cards. Visa International Law Enforcement Education Programme (2002:15) lists and explains the different types of Visa cards that are available, namely:

- Classic card;

- Platinum card;
- Business card;
- Electron card; and
- Chip card

For ethical and consent purposes, all images used in the different card figures were obtained from VISA International, who made available a compact disc (CD), which contained credit card information and credit card templates. All of the templates used in the discussion here are examples of credit cards and the account numbers and names of people imprinted on them are all fictitious.

**2.12.1.1 Visa Classic Card**

The Visa Classic card, (commonly know as the classic card) which is illustrated in Figure One, is a basic product and is the most widely used bank card in the world for purchases of goods or services (Visa International, Law Enforcement Education Programme, 2004:115). The classic card is the most common type of credit card and is usually one of several types, which is listed in point format and discussed below:

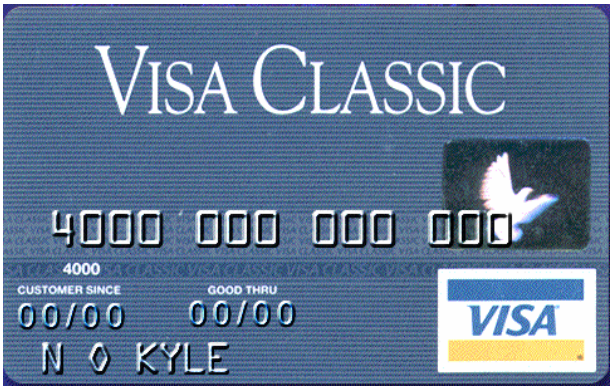
**2.12.1.2(i) Automated Teller Machine Card (Classic Card)**

The ATM card is also a debit card, as it enables withdrawals from a savings account at an automatic teller machine but does not allow charging of any outside purchase (Rapp, 1991:15). These cards are issued to individual cardholders who use the card within a limit imposed by the card issuer (Rapp, 1991:13). Up until 1983, the classic card had a common design consisting of blue, white and gold bands taking up the entire face of the card. After 1983, the Visa logo was reduced in size and along with a hologram, appears on the face of the card (Visa International Law Enforcement Education Programme, 2004:23).

When asked whether the classic cards are frequently used to commit fraud, 20 respondents indicated that the classic card is frequently used to commit fraudulent

acts and are used by opportunistic criminals, which include persons who rob one of his or her card or a person who finds a misplaced card and presents the same without altering the card in any way. Ten respondents indicated that the use of classic cards to commit fraud was frequently due to the fact that it is the most widely used card in South Africa and internationally and is carried by the majority of the population.

**Figure One: Classic Card**




.

**Visa International Law Enforcement Education Programme, 2002. Compact Disc**

**2.12.1.3(ii) Platinum Card**

The platinum card (figure two) is a global premium card and offers cardholders world classic features, such as high spending power and there are no pre-set spending limits (Visa International Law Enforcement Education Programme, 2004:115). Global premium refers to the use of the card internationally, which can be used to transact at any institution both locally and abroad and which there are no limitations or authorisation required (Rapp, 1991:12). The Visa platinum product name and unique two-part hologram must appear on the front of the Visa platinum card (Visa International Law Enforcement Education Programme, 2004:116).

Asked the question: “Are there any specific requirements to acquire a platinum card?”, five respondents stated that there is a price to pay for this card, which includes an annual fee, whilst 25 respondents stated that one is required to use the card for an amount exceeding R200 000.00 annually, or else the card is forfeited and the services terminated. These statements were verified by the researcher with the card issuers who confirmed this fact.

**Figure Two: Platinum Card**


**VISA International Law Enforcement Education Programme, 2002. Compact Disc**

**2.12.1.3(iii) Business Card**

The Visa Business Card or Corporate Card (figure three) as it is commonly known as, is issued to small business, professional markets, as well as middle and large corporations as a payment vehicle for business travel expenses. This card is issued to specific employees by the employer for their individual business related expenses (Visa International Law Enforcement Education Programme, 2004: 116). The banks have an arrangement with business and in which it allows high credit limit to company employees on the basis that the expenses incurred will be

debited to the company account and the bank is at no risk with reference to payment. Business credit cards are paid by the corporation, which provides them for its executives such as chief executive officers and directors, for example. One or more cards are often part of the prerequisites or fringe benefits that a company executive enjoys. This allows the cardholder to charge purchases and services up to a limit at the corporation's expense (Rapp, 1991:12). The card is silver grey with contrasting dark grey. The company name printed in black lettering appears on the face of the card (Visa International Law Enforcement Education Programme, 2004:117).

When asked, "How is the business expenditure on cards monitored? Twenty respondents stated that business cards issued bear the name of the employee as the account holder. The employee and the accounts department receive a statement from the bank at the end of every month, detailing the expenditure. The employee has to keep every receipt with reference to expenditure for the month. At the end of the month it is required that the employee attach all receipts as per the bank statement and complete the relevant in-house forms and forward these to the accounts department in the company. Ten respondents stated that companies employ auditors, who are responsible to conduct audits and monitor credit card expenditure on a monthly basis with reference to company credit cards.

Corporate cardholders can accrue charges up to many tens of thousands of rands, because the corporation is responsible for payment. The spending limit on the credit card is determined by company policy, which dictates the credit limit available. The card, however, can only be used for business purposes; personal use of the card constitutes fraud.

**Figure Three: Business Card**


**Visa International Law Enforcement Education Programme, 2002. Compact Disc**

**2.12.1.4(iv) Electron Card**

Traditionally, banks have managed the risks associated with new customers and those who have never had a bank account before, by requiring them to withdraw their funds in cash from a branch were they are known. Besides being inefficient for the bank, it is inconvenient for the customer (Rapp, 1991:13). The electron card (Figure four), allows the issuing bank to reduce their cost and control risks from new account holders as well as adding point of sale transactions to their existing ATM and cash withdrawal services at little or no additional risk (Rapp, 1991:14). Due to every transaction being authorised against card holders own account balance, banks can securely offer these cards to any new customer, regardless of their banking history or credit status (Visa International Law Enforcement Education Programme, 2000:17). Once the customer demonstrates the ability to manage electronic debit card accounts they can be offered other banking services (Visa International Law Enforcement Education programme, 2000:18).

Unlike other cards, the electron card can only be used if there is credit available in the account of the cardholder, which is made available by the cardholder and not

the card issuer. The electron card has no embossed account number. All electron cards display the first and last four digits of the account number; some cards depending on the issuer may have the full account number on the face of the card. In all instances the account information is laser engraved and not embossed (Visa International Law Enforcement Education programme, 2000:23).

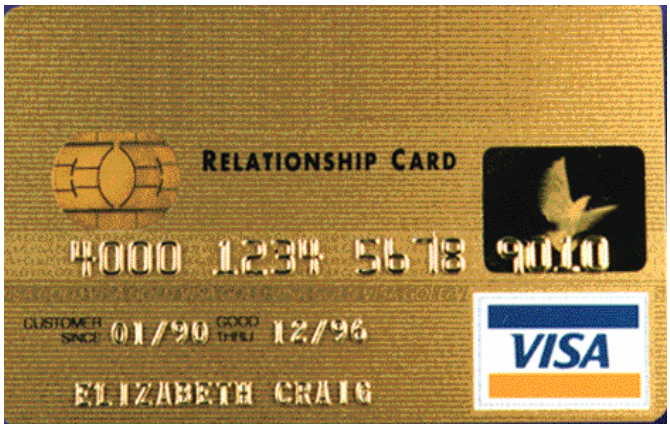
**Figure Four: Electron Card**


**Visa International Law Enforcement Education Programme, 2002. Compact Disc**

**2.12.1.5(v) Chip card (Relationship Card)**

The chip card (figure five), is a card with an imbedded integrated circuit or microchip, as opposed to the conventional magnetic stripe card (Visa International Law Enforcement Education Programme, 2004:20). This card has electronic logic to store data, and in some cases, a microprocessor, which can process data. Also known as a "smart card" or "relationship card", it can be contact (are activated when terminals touch a smart card reader) or contact less (are activated by radio waves when passed near a transmitter). The type of chip cards currently used, range from fairly simple memory devices to sophisticated microprocessors (Grabosky & Smith, 1998:159). The latest generation of chip cards contain a microprocessor, a liquid crystal display and a power source, which enables the card to be used independently of a card reader (VISA International, Law Enforcemnet Education Programme, 2004: 24).

**Figure Five: Chip Card**




**Visa International Law Enforcement Education Programme, 2002. Compact Disc**

## 2.13 Summary

This chapter addressed and explained the difference between forensic investigation and forensic science including, the crime of fraud and in particular different types of credit card fraud. The chapter further addressed credit cards issued by VISA International. It is clear that forensic science and forensic investigation are interlinked and are dependent on each other to prove or disapprove a crime or commission thereof. Credit card fraud has been committed from the time of its inception; however, modern technology and advancement have increased the ways in which it can be committed.

Upon reviewing the different explanations of credit cards including altered, stolen, lost and counterfeit cards, the credit card can be explained by the researcher as a negotiable instrument that is often used fraudulently to obtain goods and services by altering security features or the presentation of lost or stolen card. Visa, as an issuer of credit cards, has constantly reviewed its security measures that is applied to cards and devoted considerable resources to maintenance of security systems and programmes. These programs, mandated by the association include uniform card standards, security standards for the manufacturer, embossing and encoding cards, standards for mailing cards and

credit background investigations of applicants. The association's goals of constantly reviewing security methods are to create a card that is technically difficult to alter or counterfeit. It is in this light that VISA International constantly review security features in order to create security features that are unique and difficult to forge. Unique security features on credit cards are much harder to forge today than before, and new security procedures make it harder for criminals to alter these features. The following chapter will address the unique security features found on VISA credit cards.

# CHAPTER THREE
# UNIQUE SECURITY FEATURES

## 3.1 Introduction

A security feature can be defined as something distinguishable and unique in appearance (Rapp, 1991:03). The unique security features on a credit card are therefore distinguishable features that have been devised to prevent manipulation and protect all interested parties. The aim of having security features on credit cards is to prevent manipulation. The first Visa cards were of a basic design, using the Visa corporate colours of blue, white and gold as a banded card face. Apart from the printed names of Visa and the issuing member bank, the only other additions to the card were the relevant embossed details of the account number, name and expiry date. No security features were incorporated in the design of the original card. Consequently, in a relatively short period of time, counterfeit cards imitating the genuine item had been manufactured and had been widely used. Visa International Law Enforcement Education Programme (2004:65) explains that, losses in the early 1980s have amounted to millions of dollars in which counterfeit credit cards were being passed as original credit cards. Due to the sudden surge in counterfeit cards and the threat of substantial losses in the 1980s, Visa International adopted a proactive approach, which included the analysis of the product, legal and investigative assistance to determine how to go about combating the counterfeiting of credit cards (Visa International Law Enforcement Education Programme, 2004:63).

With no special features to overcome this threat, a counterfeit card could be made with little effort and provide a very likeness to a genuine card. To counteract this threat, Visa has continually added various security features to make Visa cards secure and much more difficult to criminally reproduce without detection. The current Visa card design has, through time, developed into a sophisticated anti-counterfeit product. In this chapter the researcher intends to address the concept identification. The relevance of identification to unique security features is that it

is the first step in determining whether a security feature is genuine or of a fraudulent nature. The researcher will further explain the various methods that criminals use to alter credit cards as well as explain the various security features found on credit cards.

## 3.2 Identification

Identification can be the principle that all objects in the universe are unique, because it has certain unique individual or group characteristics. It includes all relevant information, which may shed light on a case and create awareness of the possible value of every potential source of information (Marais, 1992:19). Identification means that the item shares a common source and the items can be classified or placed into groups with all other items having the same properties (Fisher, 1999:5). Generally, identification is applied by the sciences to place objects into specified groups, that is, to pinpoint an object as belonging to a specified class of objects. Lee (2000:12) explains identification as the process of using characteristics to identify a particular object. Identification generally involves one or more of the following methods (Lee, 2000:13):

- Physical measurements;
- Physical properties ;
- Chemical properties;
- Morphological (structural) characteristics;
- Biological properties; and
- Immunological properties

The purpose of identification, with reference to investigation is that physical evidence is identified, which can then be analysed and assist the investigator in pursuing a productive path by providing clues from the characteristics of the physical evidence (Lee, 2000:15).

The cumulative nature of identification is clearly reflected in the fact that a whole series of identification is sometimes required to individualise guilt or innocence.

This confirms the existence of various categories of identification. Van Heerden (1986:188) listed the following categories of identification that exist:

- Situation Identification;
- Witness Identification;
- Victim Identification; (see 3.2.1)
- Imprint identification; (see 3.2.2)
- Origin Identification;
- Action Identification; (see 3.2.3)
- Culprit Identification; (see 3.2.4)
- Cumulative Identification

For the purpose of this research, four identification categories are relevant to credit card fraud and will be discussed in more detail:

### 3.2.1 Victim Identification

This type of identification is often the most important and sometimes the only starting point to solving credit card fraud. This identification is usually based on appearance (Van Heerden, 1986:189). In credit card fraud the lawful account holder is always the victim. The victim is however always traceable, due to the fact that the banks are in possession of their personal and contact details.

### 3.2.2 Imprint Identification

The fundamental principle of imprint identification is that the distinctive characteristics of objects are transferred to the surfaces with which they come into contact (Van Heerden, 1986:189). The value of identification in this case depends upon the nature of the object and the surface upon which the imprint was made. In credit card fraud the fingerprints of the suspect is always left on the credit card.

### 3.2.3 Action Identification

This type of identification refers to the identification of human acts that are directly related to the crime and indeed form its central element (Van Heerden,

1986:190). This category becomes relevant with regards to crimes such as fraud, forgery and uttering or any other crime or incidence where a disputed document is either directly involved in its commission or could be an important and revealing clue. A fraudulent credit card is categorised as a disputed document and therefore, action identification assists in determining whether the card is genuine or not by examining its security features.

### 3.2.4 Culprit Identification

This form of identification is concerned with the positive identification of the perpetrator as a person rather than the identification of the unlawful conduct (Van Heerden, 1986:190). It involves techniques such as personal description, sketches, identification and modus operandi. In credit card fraud the identity of the offender is crucial in providing information as to how they came in possession of a lost/stolen card or a counterfeit card.

## 3.3 Altered Credit Cards

Genuine credit cards can be altered. A card that has been modified to reflect a different name, account number, expiration date and/or signature other than that of an original card either by altering or re-embossing the details on the face of a card. Re-embossing is a process of placing identifying data on a bank card in the form of raised characters on the face of the card, or by re-encoding information on the magnetic stripe on the back of the card. Lost or stolen cards allows criminals to take advantage of the genuine security features on the cards, however alterations to the card and the security features can be detected by careful examination of the card (Visa International Law Enforcement Programme, 2000:16).

### 3.3.1 Re-embossing

Re-embossing can change details such as the account number, name and expiry date on the front of the card. This process requires the legitimate embossing to be flattened allowing the criminal to re-emboss the card with new information.

However, this crude alteration method is easily detected by close examination of the card. The old embossed details can be seen as ghost images under the new number. The hologram might be distorted if heat was applied in that area. Re-embossed credit cards can only be used in a transaction where a manual imprinter is used or where the account number is manually entered at an electronic point-of-sale terminal. The four digit printed bin will always be different from the first four digits of the account number (Visa International Law Enforcement Education Programme, 2000:18).

### 3.3.2 Re-encoding

The second method of altering a credit card is by re-encoding new account information onto a magnetic stripe. The magnetic stripe contains the account number, expiry date and special security information that allow a transaction to be processed through an electronic point of sales terminal. While there may be no visible traces of the alterations of the magnetic stripe should a genuine card be used, the printed transaction voucher will show a different account number to that embossed on the face of the card. However, if the card was a true counterfeit the embossed account number will match that on the electronically printed account voucher (Rapp, 1991:15). To the question what changes to a credit card did you as an investigator experience during your investigation of credit card fraud, 20 respondents indicated that the most common changes are related to re-embossing whilst 10 respondents indicated re-encoding of information onto a magnetic stripe.

## 3.4 Security Features on a Credit Card

The term “feature” is defined as a distinctive aspect or element or a prominent aspect of something (Concise Oxford School Dictionary, 2002:121, 321). The best a credit card security officer can hope for is to make it difficult enough for fraud artists that they will find it unproductive to try to carry out any fraud (Grabosky & Smith, 1998:18). What actually happens, though, is that a small number still try and often succeed. The reason is that each new security feature suggests a new

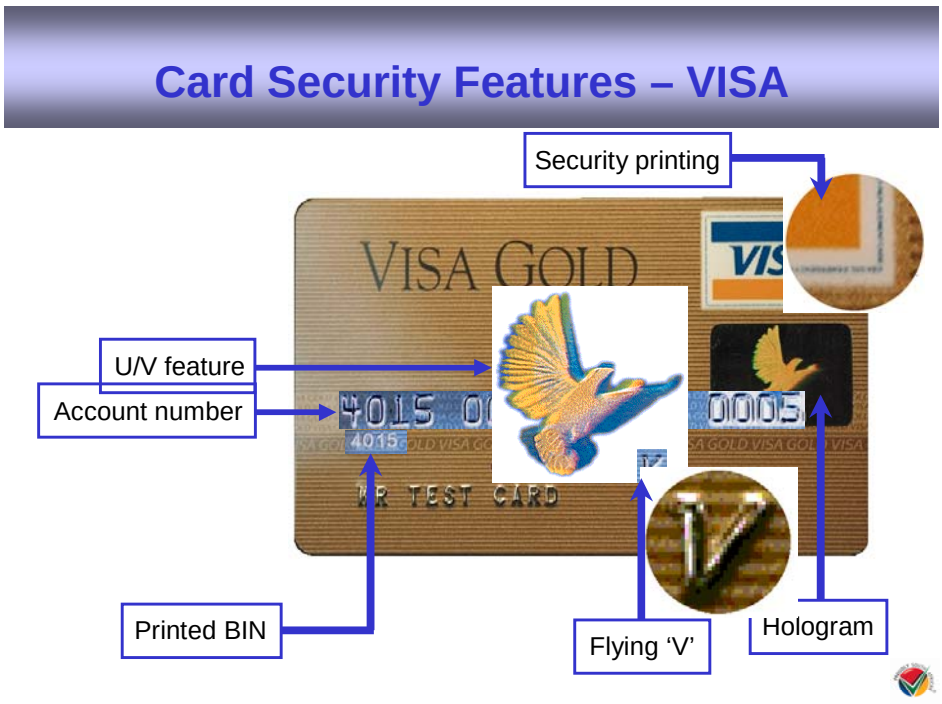
way to defeat it (Rapp, 1991:22). Security features are becoming more rigorous. Credit cards today are much harder to forge than before, and new security procedures make it harder to misuse a lost or stolen card. The term feature is defined as a distinctive aspect or element or a prominent aspect of something (Concise Oxford School Dictionary, 2002:121,321). Over the past 20 years there has been a constant race between the credit card industry developing new security features to deter counterfeiting and the criminals working hard to compromise the technology and manufacture counterfeit cards.

To defeat counterfeiting attempts, bankcards in particular began sporting an assortment of security features, such as complex and colourful designs, fine line printing, unique embossed features, holograms, ultra violet printing and tamper resistant signature panels. The advent of electronic data capture added further security to bank cards as card identity information was encoded onto magnetic stripe. This, however, did not deter criminals. Aided by improvements in multi-colour printing, laser printing and digital imaging, criminals began to manipulate credit card security features.

The discussion which follows explains how stolen, lost and counterfeit credit cards are used by criminals to perpetrate fraudulent acts. Security features on credit cards are situated on the front of the card as well as on the back of the card. The discussion will, therefore, be divided into those two categories. The following security features are found on the front of a credit card:

### 3.4.1 Security Features on the Face of a Credit Card

**Figure six: Card Security Features - VISA**




**(Visa International Law Enforcement Programme, 2000: 12).**

#### 3.4.1.1 Hologram

Rapp (1991:27) explains that holograms are small metallic oblongs, containing a laser-etched image on their surface. The image changes shape and colour depending on the viewing angle, and is very difficult to forge. The most visual feature on a credit card is the three dimensional hologram of a dove that is situated at the right hand side of the front of the card. When the card is tilted the hologram will give an impression of movement in the dove's wingtips and show a change of colour. The last four digits of the embossed account number are incorporated in the hologram (Visa International Law Enforcement Education Programme, 2000:29).

Very few "counterfeit holograms", have actually been used. In most cases of counterfeit cards, the hologram is not a hologram but a look-a-like item that is

"reflective" rather than "refractive". Holograms are refractive, that is, the item in the hologram appears to actually move, whereas a reflective item is only a photo on a reflective material. Forged holograms have included printed images using a variety of materials and inks. Some have used plain foils and or diffraction grating foils (Visa International Law Enforcement Education Programme, 2000:30).

When asked "how does one check for a counterfeit or suspect hologram?", 13 respondents indicated that the best way to check a suspected hologram is to compare it to a card you know to be genuine, whilst 17 respondents indicated that the card should be tilted and one must be able to see movement in the wingtips and change of colour. During interviews conducted all respondents were familiar with the hologram as a security feature. This was determined by the researcher receiving the same type of response from all participants which resulted in saturation levels being achieved.

The manipulated hologram security feature represents misrepresentation by being passed as the original. Many attempts have been made by criminals to replicate holograms but there have been a number of differences when compared to the original. Fraudulent holograms comprise flat images of a dove which includes no movement or colour change. The image of a dove is stamped onto foil to create a dove image (Rapp, 1991:23).

#### 3.4.1.2 Security Printing

At the top, right (front) corner of all Visa cards is the Visa logo. Surrounding the logo is a security feature known as security printing (micro printing). This fine line printing, only distinguishable through magnification, is an alpha numeric repeated sequence providing specific identification and verification details, including the type of product and the card printer of the card (Visa International Law Enforcement Education Programme, 2000:31). Rapp (1991:25) indicates that micro printing is extremely small printing, too small for the naked eye, and is very difficult to copy or reproduce by technical means. Asked the question whether

micro-printing can be tampered with or compromised, 18 respondents indicated that criminals use a method known as “shave and paste”. This involves carefully shaving the fine line printing of the plastic with a sharp razor blade and then pasting on a new fine line printing or a resemblance thereof by using special liquid glue. Twelve respondents stated that criminals attempt to reproduce micro printing via a photocopy machine and, upon inspection, a solid line is noticed.

Security printing (micro printing) of a fraudulent nature differs from the genuine as it does not include the first four digits of the account number as well as other security information. A thin line appears and no printing is present. The lines are either dotted or solid and no fine line printing exists as is required (Visa International, Law Enforcement Education Programme, 2000:31).

#### 3.4.1.3 Ultraviolet Dove

In the centre on the front of the card there is an ultraviolet security feature. In the centre on the front of the card and over part of the account number below the expiry date, is the ultraviolet (u/v) feature. A fluorescent image of a dove will be seen when ultra violet light is passed over the face of the card. This image is a completely different dove and not the same as is found in the hologram. Criminals do not interfere with this security feature and in many cases, they are not knowledgeable about the existence of the security feature (Visa International Law Enforcement Education Programme, 2000:32). Rapp (1991:25) states that some cheques and credit cards have images or symbols printed in ultraviolet ink. These are invisible to the naked eye in normal light but show up very clearly under ultraviolet light. Asked the question, “from your experience, can the security feature be tampered with”? All respondents indicated that according to their experience this security feature has never been tampered with.

#### 3.4.1.4 Printed Bin

Another highly visible security feature is the printed bin situated below the first four digits of the account number. This is a four digit printed number that matched

the first four digits of the embossed account number. The “printed bin”, will be either above or below the start of the embossed account number. This printed bin is the bank’s identification number (Visa International Law Enforcement Education Programme, 2000:32).

Asked the question, “from experience can the printed bin as a security feature be tampered with”? All 30 respondents stated that the printed bin, as a security feature, can be tampered with. Asked the question, “what method do criminals use to manipulate the printed bin as a security feature”? Seventeen respondents explained from their experience that criminals usually use a method known as shave and paste, which requires the careful shaving off the details using a sharp instrument, for example, a razor blade, and then place new details affixing it to the card by using special liquid glue. Thirteen respondents stated that criminals also use a method known as re-embossing, a process that requires the legitimate embossing to be flattened allowing the criminal to re-emboss the card with new information.

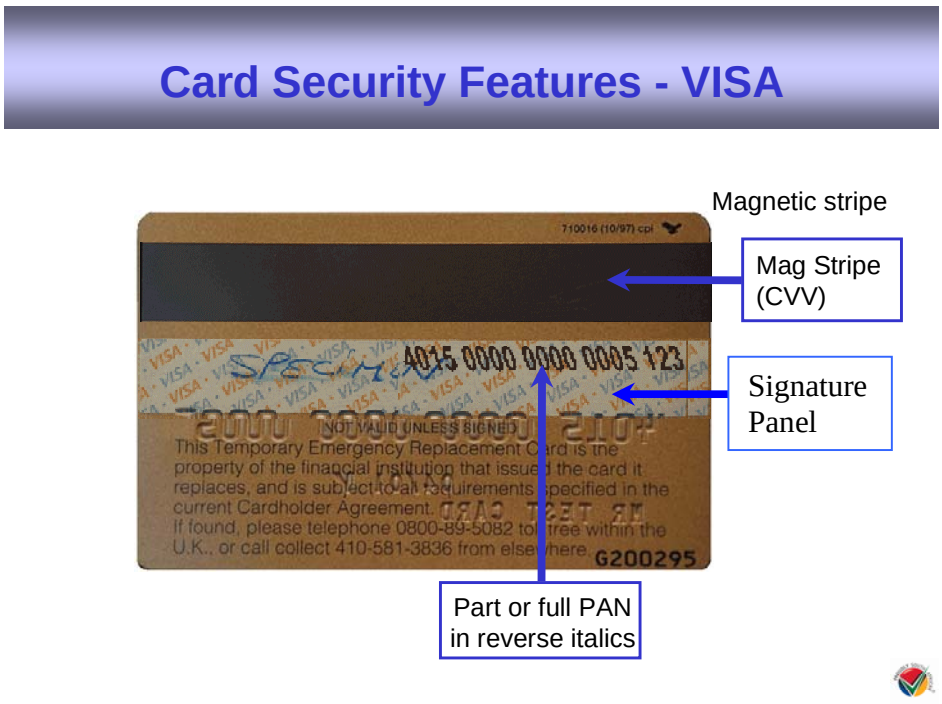
#### 3.4.1.5 VISA V

Immediately after the expiry date on the front of the card there is a special single embossed security character, commonly referred to as the “Flying V”. The embossing die set required to emboss this feature is strictly controlled by VISA. The VISA V is embossed at a 45 degree angle (Visa International Law Enforcement Education Programme, 2000:33).

When asked, judging from their experience, how the Flying V has been manipulated, 18 respondents stated that the Flying V is usually manipulated by a technique known as “shave and paste” and on counterfeit cards, the manipulated Flying V, is never at a 45-degree angle. Seven respondents indicated that the manipulated Flying V is not on the same line as the valid dates. Five respondents indicated that the Flying V on counterfeit cards is at times embossed in an up-side down manner.

### 3.4.2 Security Features on the Back of the Card.

**Figure Seven: Card Security Features - VISA**




**(Visa International Law Enforcement Education Programme, 2000:20).**

#### 3.4.2.1 Magnetic Stripe

A magnetic stripe is a stripe of magnetic tape affixed to the back of a card. The magnetic stripe contains essential cardholder and account information. The magnetic stripe can store about 130 characters or numbers. The magnetic stripe allows a transaction to be processed when it is read at an electronic point of sale at a merchant. The information includes the account number and expiry date, which must correspond with those embossed on the face of the card (Visa International Law Enforcement Education Programme, 2000:33). Gup (1995:120) explains that the use of non-standard stripes makes it difficult for a forger to encode information onto the magnetic stripe. Although it is technically possible to remove a magnetic stripe from a card and replace it with another, or re-record

over it, in practice, it is uneconomical. Rapp (1991:27) explains that a magnetic stripe includes the painting of a stripe of magnetic ink on the back of a card which allows for the recording of information that only a magnetic reader can read. When asked, "how magnetic stripes can be manipulated"? Twelve respondents indicated that the magnetic stripe can be removed from the card and replaced with another. Eighteen respondents indicated that the magnetic stripe can be re-recorded.

#### 3.4.2.2 Card Verification Value

The Card Verification Value (CVV) is an algorithmically calculated number that is verified by the issuing bank when a transaction is completed through an electronic point of sale terminal and appears on the back of the card (Visa international Law Enforcement Education Programme, 2000:12). The check allows the bank to confirm that the information is the same as that encoded on the magnetic stripe of the genuine card. To counter the threat of encoded counterfeit cards, the industry began to encode special information on the magnetic stripe of all valid cards. This number is based on the account number, expiration date and service code, and is calculated (Visa International Law Enforcement Education Programme, 2000:34). When asked, "how can the card verification value as a security feature be manipulated"? All respondents indicated that the card verification value is automatically compromised or damaged when the magnetic stripe is tampered with.

#### 3.4.2.3 Signature Panel

The signature panel has the word "Visa" in blue and gold at 45 degrees on a white background and appears on the back of the card. If the panel is tampered with, to remove a genuine signature, the word "void" will show through. The genuine cardholder is required to sign the signature panel on receipt of the card. With the exception of transactions where it is permissible for the card to be absent, in mail or telephone orders, the signature on the card is normally checked by merchants against the signed sales voucher at the time of purchase to verify the genuine

cardholder is using the card (Visa International Law Enforcement Education Programme, 2000:34). The earliest method of ensuring security was to have the cardholder sign the card upon receipt, for comparison with the signature on the credit card receipt slip for each purchase. This was not a very effective security measure, but it continued until better means arrived (Grabosky & Smith, 1998:321). According to (Rapp, 1991:22), some people are skilled in signature forgery and they gravitated naturally towards crimes involving such forgeries. This is based on the fact that people often sign their names differently because of fatigue, illness and other factors. Chemical eradicators allowed some card criminals to remove the legitimate signature from a stolen or lost card and substitute their own. This made it necessary to over print a signature strip with a light coloured pattern using a special ink that would change colour when it came in contact with an ink eradicator. The ink would also rub off if any attempts were made to remove the signature with a rubber eraser (Rapp, 1991:22). Respondents were asked, "what measures are put in place to verify signatures when credit cards are tendered as a method of payment"? All 30 respondents indicated that all that was required by the person receiving the card was to confirm that the signatures on the cash sales receipt corresponded with that of the card, and that, if necessary, the card is placed under an ultraviolet light to determine if the signature strip is genuine and not tampered with. Then the signature on the card is compared to that on the cash sales invoice.

#### 3.4.2.4 Card Verification Value 2

On the panel of the card is a reverse-inclined, indented printed number, known as the Card Verification Value 2 (CCV2). Part of this number is an algorithmically calculation which the issuer can verify as genuine. The value can be checked when a merchant is required to refer to the issuer of an account for authorisation of a transaction where an electronic approval is not available or permissible (Visa International Law Enforcement Education Programme, 2000:36). Asked, "how the CCV2 security feature can be altered or manipulated"? All respondents indicated that this security feature cannot be altered due to the fact that when the

signature panel is tampered with, the CCV2 is automatically damaged or compromised.

### 3.5 Summary

Credit card issuers and card associations have devised a variety of security features to deter thefts and counterfeiting. These features include holograms, graphics, unique account numbers and validation codes, embedded computer chips and other features. Thus, the technology of credit cards is becoming an increasingly important deterrent. After each technological innovation is introduced, it takes time for fraudsters to overcome the new obstacle. When they succeed the credit card industry must escalate the level of technology. Each escalation raises the cost and level of sophistication needed for counterfeiting credit cards. It also raises the cost for legitimate credit card users and merchants.

Security measures are becoming more rigorous. Credit cards today are much more difficult to forge than before and new security procedures and measures make it harder to misuse a lost or stolen card. While preventing card losses and counterfeiting difficult to control due to a high number of vulnerable points, there is reasonable hope in preventing these cases of fraud. Giant financial companies, such as Visa International, have taken steps to protect themselves. Prevention is the key to reducing plastic counterfeiting, theft and misuse of credit cards which can be achieved by meaningful partnerships being forged between the industry, merchants, and law enforcement agencies.

# CHAPTER FOUR
# PREVENTATIVE COUNTERMEASURES

## 4.1 Introduction

The enormous growth of credit cards has left many law enforcement agencies with mixed emotions. On the one hand, a certain number of people see credit cards as creating a whole new field of criminal activity that is extremely difficult to control. On the other hand, many police agencies have realised that investigation into this crime can provide a useful tool for detecting and apprehending criminals and also to identify measures that can be taken or put in place to prevent such fraudulent acts and behaviour, which will result in the prevention of these crimes (Visa International Law Enforcement Education programme, 2004:120). The role that investigation plays in crime prevention is to create awareness, as well as introduce preventative measures to counteract fraudulent activity perpetrated by criminals, as well as the apprehension of the fraudulent credit card user. Investigations into credit card fraud have provided vital evidence during the investigation of burglary, robbery or even murder. Investigations have revealed that criminals perpetrating these crimes are experts in their field in that they do their homework on financial systems and identify weaknesses in systems that allow them access to millions of rands.

Gup (1995:126) explains that the attacks and criminal successes of credit card fraudsters are more often than not the result of careful planning, precise execution of the scheme and ultimately taking advantage of financial systems originally designed to be consumer or customer friendly. Investigations have thus revealed criminal trends and practices, which result in the relevant authorities putting in place preventative counter-measures to combat this illegal activity. Credit card issuers have explored a variety of preventative alternatives over the years. A number of these alternatives have, however become outdated, as criminals have adopted sophisticated methods to perpetrate credit card fraud. The only hope to combat these criminal activities is through intensive investigations, which will

lead to the adoption of, and implementation of preventative measures based on the findings from investigations.

Part of the responsibilities of a corporate investigator is to report and formulate preventative measures to management. It is for this reason that this chapter is included in this study.

## 4.2 Preventative Countermeasures

Preventative countermeasures refer to steps taken by organizations to protect themselves against criminal activities (Rapp, 1991:71). A person will only commit a crime if he or she believes that the benefit will out-weigh the risks, so by showing what happened to criminals (increase awareness), knowing that committing a crime is not worth the risks, will become a part of a culture in a country. Ever since plastic cards were introduced attempts have been made to steal them, counterfeit them or otherwise misuse them in order to obtain funds illegally. Unfortunately, it is not possible to offer a simple or foolproof solution to prevent credit card fraud. While the root causes are fairly constant the means, schemes and motives of the perpetrators vary.

Preventative countermeasures will look to address successful monitoring techniques and provide a basic understanding of circumstances that have repeatedly proven to expose companies to the potential of credit card fraud. It will further provide steps (preventative countermeasures) that can be implemented to successfully counteract credit card fraud. Sources consulted during the research of this dissertation suggested a number of preventative countermeasures. These are;

- Personal Alertness;
- Retail Precautions;
- Background Checks;
- Keeping competent hired employees; and
- Security at the cash register

Each of these measures will be discussed separately.

### 4.2.1 Personnel Alertness

Combating credit card fraud often begins with the cardholder, who should report immediately any loss or theft of credit cards. It is as important as safeguarding one's card to reduce the opportunity for theft (Rapp, 1991:72). Asked, "how should members of the public safeguard their credit cards from theft and other criminal acts"? Twelve respondents stated that the card should at all times be kept in a safe place, such as, a wallet and not in one's pocket, as well as ensure that lost or stolen cards are reported immediately. Ten respondents stated that the card should never be left unattended and that expired cards should be destroyed immediately to avoid the card being used as a counterfeit card and prevent the criminal obtaining the card details. Eight respondents stated that the public must think of credit cards as "physical cash" and must carry cards that they will need and ensure that new cards are signed immediately.

Grabosky and Smith (1998:169) stresses the need for members of the banking public to realise that the plastic card and secret identity pin represents their electronic signature. Protection of "pin numbers" is a primary crime prevention strategy. Plastic cardholders are best placed to protect themselves by taking basic security precautions to ensure that their cards are not stolen. This includes not leaving them in public places and ensuring that they are reclaimed after use. Consumers are also advised not to compromise their security by disclosing "pin numbers", keeping pin numbers with cards or writing them on cards (Grabosky & Smith, 1998:170). Asked "how a person could protect their pin number"? Twenty respondents stated that, in-order to protect one's pin, one has to memorise it. Ten respondents stated that cardholders must be vigilant at ATM machines and must not accept help from strangers when encountering difficulty at an ATM machine.

Killick (1998:121) states that one of the most effective strategies used to control credit card fraud is to educate the public as to the nature of the security risks,

which they face and how they can protect themselves. He goes on to recommend that financial institutions use audio and visual electronic media to publicise the need for security such as utilising community service announcements on radio or television. When asked "what proactive measures are in place to educate the public on credit card fraud"? All respondents indicated that VISA and all the major banking institutions in the country have implemented an effective card (fraud??) prevention strategy called "card-watch". This involves a high profile publicity and education campaign, which includes posters, leaflets, television and radio coverage, to raise public awareness of the problem and to encourage card holders to take more care of their cards.

Investigators always interact with complainants on a regular basis and therefore can be considered as the best instrument to be used in educating the public/complainant. The education process can include an informal workshop on personal alertness, lasting approximately five minutes, during which the complainant is made aware of credit card security and the importance of keeping their pin number safe and why they should safeguard their card at all times (South African Police Service, Advance Training Manual, Commercial Crime, 2002:08).

### 4.2.2 Retail Precautions

Retailers deal directly with people, both their employees and clients, which make the human factor the most important one in the equation. Hiring and keeping good people is an important first step, which many employees neglect (Rapp, 1991:72). Killick (1998:112) states that there are two important parts to staffing with competent people. The first is hiring. It is important to hire intelligent and honest people at the outset by conducting thorough checks on the applicants to avoid the possibility of hiring undesirables. The second is compensating staff adequately in terms of salary. When asked what preventative measures are in place in the banking industry to curb credit card fraud, respondents from the South African Police Service and Nami-Tech indicated that they were not knowledgeable about

the banking industry's strategy on prevention, and, therefore, were not in a position to answer the question. Of the 12 respondents from the banking industry, six respondents stated that staff is continuously attending workshops and courses relating to credit card fraud. Four respondents stated that members of staff who identify fraudulent credit card transactions are rewarded financially. Two respondents stated that staff is subjected on a yearly basis to polygraph testing in order to determine their trustworthiness to the company. It is also important that the investigator also play an important role in this respect by, on a regular basis visiting stores and coming into personal contact with personnel in order to create awareness and make staff aware of their presence (South African Police, Detective Training Manual 2004:26).

### 4.2.3 Background Checks

Background checks both on future cardholders and on personnel can be considered as the oldest of prevention strategies. Only background checks can verify the statements made in the employment application or the answers to the interviewer's questions (Rapp, 1991:73). Grabosky and Smith (1998:164) explain that a major point, which many employers and interviewers miss, is that the information contained in the application and the candidate's answers to interview questions must be verifiable. Financial institutions are able to adopt a wide variety of self-help strategies with reference to background checks, which may reduce the risk of credit card fraud. First, they need help to adopt in-house security procedures and to ensure that staff is checked for security breeches, as credit card fraud often requires the involvement of confederates with inside knowledge of the institutions' security and computer procedures (Visa International Law Enforcement Education Programme, 2000:73). When asked "what procedure is in place with reference to background checks on bank employees"? Respondents from Nami-Tech and the SAPS were unable to answer this question due to them not knowing the policy banks employ when recruiting staff. From the sample of 12 respondents from the bank, eight respondents stated that apart from the company carrying out its own investigation on an employee's background,

companies are also using bodies such as Kroll MIE (a company that specialises in researching the background of potential employees and which include criminal, civil, and ITC checks. Four respondents stated that background checks, when employing individuals, are not only limited to the individual, but includes checking the background of parents, brothers, sisters, etc. All respondents stated that it is prudent and vital that there exist a close working relationship between corporate investigators and human resources departments.

### 4.2.4 Keeping Competent Employees

A background check is, however, not enough. Hiring good people is not the same as keeping them. Employees who feel that management treats them fairly would not harbour any smouldering resentment that an exploitative relationship might foster (Grabosky & Smith, 1998:112). It is in this light that it is important for the employer or manager to concentrate on the big picture, instead on the narrow view of one authority who describes security efforts in terms such as "putting pressure" on dishonest employees. Bologna (1984:11) explains that the unwillingness to provide adequate salaries and benefits does not really save money in the long run and, instead, such a policy has several effects, some which show up immediately and others which appear later.

Rapp (1999:75) points out that reasons why employees collude with criminals in committing credit card fraud include the following:

- Many qualified applicants lose interest in a position which pays less than that offered by another company;
- Those who remain interested in the position are the less qualified ones who usually collude with criminals in committing crimes against their employers;
- If the applicant for a low paying job appears qualified he may accept the job only because of immediate financial need and will constantly be seeking better employment. The second possibility is more sinister, the seemingly qualified applicant has a hidden agenda, perhaps seeking to

become the “inside man” for a credit card syndicate, where he could accept counterfeit and stolen credit cards for purchases from syndicates.

The enlightened employer who understands that loyalty is a two way street, will get more from his employees, especially if they pay high enough salaries and give their employees a vested interest in keeping their jobs, knowing they won’t easily be able to find another position with the same salary and benefits. This builds a sense of commitment and willingness to perform to keep the job. This includes observing security measures against credit card fraudsters (Corner, 2003:32). When asked “of what benefit is competent staff to a company”? Twelve respondents indicated that employing competent staff can be regarded as a preventative measure, because they are in a position to identify fraudulent cards and prevent the illegal act immediately. Eighteen respondents indicated that due to competent and vigilant staff, criminals have become aware of this and rarely commit crimes in these environments because the risk factor in getting caught is high. When asked “how important is it to educate staff on credit card fraud”? All investigators stated that it is imperative and of the utmost importance that staff be educated and that they personally play a role in educating staff. Twelve investigators indicated that workshops be held every three months educating staff on security features and the new modus operandi practised by fraudsters with reference to credit card fraud. Fourteen investigators stated that businesses must be visited personally and staff must be presented with a half-an-hour presentation on the new trends and modus operandi being practised by fraudsters. All investigators recommended that CD’s be put together on a regular basis containing updated information on security features, crime patterns, and any other relevant information about card fraud in particular. This can then be distributed to staff regularly and can serve as in-house training.

### 4.2.5 Security at the Cash Register

Rapp (1991:76) states that there are several precautions a merchant and his employees can take to make life harder for the fraudulent credit card presented by fraudsters:

- person receiving the card must compare signatures on the cards and the cash receipts.

  When asked, how reliable is the preventative measure of comparing signatures on the card to the cash receipt? 11 respondents stated that it is not foolproof but it will stop a percentage of fraudulent cards being presented. The reason for it not being foolproof is attributed to the fact that a skilled fraudster can paint over the signature strip on a credit card and sign it. The professional credit card fraudster obtains new unsigned credit cards (duplicate credit cards) and signs them before presenting them at different outlets (Visa International Law Enforcement Education Programme, 2000:18). Nineteen respondents stated that it is the most common preventative measure and the most important preventative measure because it indicates to the fraudster that he is dealing with competent and trained individuals.

- Check the expiration dates religiously:

  When asked "why is it important to check expiry dates"? Four respondents stated that it prevents the passing of expired cards. By checking the dates and signatures on the card the shop will become known as being vigilant and alert and criminals will avoid doing business at that particular business. Twenty six respondents stated that the expiration date can also reveal a new card and becomes suspicious when the customer is making large purchases with it. The person presenting the card may have stolen it from a post box or pick pocketed someone. The person receiving the card and more especially the credit card investigator must look for signs of forgery or alterations. These may include:

  - Missing logos;
  - Chipped or peeling panels;

- Warped plastic;
- Erasures;
- Alteration of the signatures; and
- Embossed name does not match the signatures.

- The person receiving the card must request for additional identity.

  When asked, "what is the reason for requesting additional identity"? Nineteen respondents indicated that this is the only partial measure against professional credit card fraudsters, because fraudsters come equipped with supporting documents. Recording this additional information can help spot fraudulent users. Eleven respondents stated that the reason is that although a fraudulent user may change credit cards often, even daily, he or she is less likely to change their supporting documents often. Gup (1995:104) explains that it is also helpful for cashiers and bank tellers to be vigilant for behaviour fitting this behavioural profile, because this can signify the possibility if card fraud. Customers that appear excessively nervous and who carry the card in a pocket instead of a wallet must also be observed and watched.

### 4.3 Alternative Preventative Measures

One of the greatest areas of risk associated with the use of plastic cards relates to the manner in which cardholders' identities are verified. Visa International Law Enforcement Education Programme (2000:85) provides some of the most recent suggestions for improving security in this area, which includes the use of cards which have:

- a photograph of the user;
- laser engraved signatures;
- larger PINS;
- various biometric means of verifying identity, such as a signature; and
- fingerprints, palm, lip, ear, or retina scanning

These measures however are still in the trial phase and have not been implemented nor are there any cards with these features available. Asked, what preventative countermeasures can you suggest to improve the security of credit cards? 10 respondents stated that all stores should be equipped with closed circuit television (CCTV), which would allow security personnel to monitor suspicious movements of criminals and also record their fraudulent acts and, most importantly, they will be to identify the perpetrator even if the perpetrator avoids arrest. Nine respondents stated that training cashiers to identify fraudulent security features should be considered the most important. Seven respondents stated that substantive financial rewards should be made available to persons who identify fraudulent cards, which will result in awareness and vigilance by persons who receive fraudulent cards as method of payment. Four respondents indicated that special task teams from the SAPS be deployed to investigate credit card fraud as well as specialist prosecutors prosecute the cases.

## 4.4 Summary

The solution to credit card crime will ultimately depend upon the adoption of a range of mechanisms between all those involved in providing and using systems. This includes telecommunication carriers, service providers, financial institutions, retail merchants and individual users. The key to reducing credit card crime and disrupting criminals is the establishment of a meaningful partnership between the credit card industry, merchants and law enforcement agencies. Card payment systems and their affiliated financial institutions must be prepared to exchange pertinent, sensitive and timely information with law enforcement agencies to enable them to target corrupt merchants and other organised criminals involved in plastic counterfeiting, productively.

# CHAPTER FIVE
# FINDINGS AND RECOMMENDATIONS

## 5.1.1 Introduction

The research for this dissertation was borne out of the need to improve the general knowledge of investigators, specifically those investigating crimes where credit cards are involved. The research focused around the unique security features of a credit card with the aim of identifying how these cards could be used fraudulently. In these cases the credit card is the centre of the investigation and can be used as an exhibit as well as a crime scene, if the Locard Principle is applied. To ensure that investigations are successful and the perpetrators of card fraud are caught, it is imperative that investigators are knowledgeable and well trained in identifying those security features on credit cards that are not genuine and are of a fraudulent nature. From experience, investigators do not examine fraudulent credit cards thoroughly to determine possible crimes in respect of fraudulent security features that are endorsed therein, but charge the suspect with the first and most obvious crime that they identify and in many cases the signature on the card is the most obvious security feature breached in terms of fraud.

To address these shortcomings, the aim of the research was to research the unique security features of credit cards and identify possible fraudulent use. To address this aim, three research questions were asked, namely:

- What is meant by the concept credit card?
- What are the unique security features of a credit card?
- What preventative counter measures can be taken to prevent fraudulent manipulation of the security features on a credit card?

In an attempt to address the research questions the researcher gathered information from literature by authors of national and international origin, and also involved the experience of investigators to obtain knowledge from practice.

## 5.2 Findings

The following findings related to the research questions based on information obtained from the control group of respondents and from view points of national and international sources are indicated below.

### 5.2.1 Research Question One

What is meant by the concept credit card?

During the research it was established that:

- A credit card is a financial transaction card that allows the cardholder to obtain money, goods or services under a line of credit established by the card issuer.
- Not all respondents had a clear understanding about the difference between a debit card and a credit card. Twelve respondents assumed that a debit card falls in the category of credit cards.
- All respondents were familiar with the concept credit card and the functions thereof.
- There is, however, limited information with reference to security features of credit cards.

### 5.2.2 Research Question Two

What are the unique features of a credit card?

During the research it was established that:

- The unique security features of a credit card are distinguishable features that have been devised to prevent manipulation and combat fraudulent activity.
- Not all respondents were familiar with all the security features endorsed on a credit card. The following security features are found on a VISA credit card, namely:
    - Security Printing;
    - Ultra Violet feature (flying dove);
    - Account number;

- Printed bin;
- Hologram;
- Flying V;
- Magnetic stripe;
- Card verification value;
- Card verification value 2; and
- Signature panel.

- Sixteen respondents were not familiar with the ultra violet dove and the Card Verification Value 2 (CCV2) feature. This is attributed to the fact that these are hidden features embedded in the card which are not visible to the naked eye.

### 5.2.3 Research Question Three

What preventative measures can be taken to prevent fraudulent manipulation of a credit card? It was established that preventative measures to prevent fraudulent manipulation could include:

- technological advancement, especially the introduction of the micro-chip as a security feature, which can be embedded in credit cards;
- awareness campaigns involving the education and training of both the public and investigators;
- Offering of a cash reward scheme to all persons who identify fraudulent cards when presented to them to process a transaction;

## 5.3 Secondary Findings

The following findings were made in terms of certain other relevant points that the researcher came upon during the research:

### 5.3.1 Objective of Forensic Investigation

- It was found that the objectives of a forensic investigation are to establish if a crime has actually been committed, to identify and apprehend the

suspects, to gather and safely keep evidence, recover stolen property, and to assist in the prosecution of the person charged with the crime.

- All the respondents were not certain about the objectives of forensic investigation.

### 5.3.2 Mandate to Investigate

- The researcher established that the South African Police Service (SAPS), The Directorate of Special Operations (DSO), the Special investigating Unit (SIU), corporate investigators and private investigators have a legal mandate to investigate cases. However, if any organisation apart from the DSO wants to institute criminal action it would have to involve the SAPS.

### 5.3.3 Purpose of Identification

- It has been established that identification means that all objects are unique because it has certain individual or group characteristics, for example, the print on a credit card is a fingerprint of a person, but it does not prove which person committed the crime.
- The purpose of identification includes; establishing the elements of the crime; the type of crime committed; the clues, information and evidence pointing to the crime; and establishing the identity of the perpetrator of the crime.

  Eight respondents were familiar with the purpose of identification whilst the remainder of respondents were unclear as to the purpose identification.

## 5.4 Recommendations

At the beginning of the research report it was stated that the purpose was to develop a good practice and to empower and enhance the performance of individuals involved in investigation. This can only be achieved if investigators are knowledgeable and have a proper understanding of what they were investigating.

The research has addressed a variety of concepts based on the research questions and aims which were discussed. There are not much literature available on some of the concepts and partly due to that, there is a lack of knowledge amongst investigators which has serious implications for investigations.

For the purpose of clarity more research is required in the following areas:

- Forensic investigation, its purpose and objectives;
- Establishing the difference between identification and individualisation; and
- Mandate to investigate.

To enhance the investigation skills and improve the knowledge of investigators regarding the investigation process, it is recommended that the training curricula for investigators, both in the SAPS and the private or corporate sectors, address the following:

- the nature and purpose of forensic investigations;
- Identification;
- the Locard Principle;
- Credit cards (security features);
- Preventative measures
- credit card fraud.

## 5.5 Summary

The aim of this research project was to identify fraudulent security features on credit cards used by VISA International. It is evident that the information on this topic is limited and that more research is required on the unique security features of a credit card in order to support education and training in this field. It is evident from the findings of this research project that the respondents (investigators) have various shortcomings in respect of identifying all the security features endorsed on the credit cards, especially those features that are not visible to the naked eye.

These shortcomings may lead to the failure to identify fraudulent security features when investigators are presented with cases to investigate.

The researcher hopes that this research will empower investigators with the knowledge needed to enhance their performance and ability to investigate credit card fraud cases much more successfully.