## IN THE HIGH COURT OF SOUTH AFRICA (DURBAN AND COAST LOCAL DIVISION)

**CASE NUMBER: 2000/3156** 

In the matter between:

**DINERS CLUB SA (PTY) LIMITED** 

**Plaintiff** 

and

SINGH, ANIL

First Defendant

SINGH, VANITHA

Second Defendant

# PLAINTIFF'S NOTICE IN TERMS OF RULE 36(9)(a) AND (b) IN RESPECT OF THE TESTIMONY OF PETRUS ADRIANUS BONFRER

TAKE NOTICE that

#### PETRUS ADRIANUS BONFRER

will, at the hearing of the trial in this matter, give expert evidence on behalf of the plaintiff as hereinafter set forth.

TAKE NOTICE FURTHER that the testimony of **PETRUS ADRIANUS BONFRER** will be as hereinafter set forth.

#### **INTRODUCTION**

ţ,

#### The expert's experience and qualifications

- The expert commenced employment with The Trust Bank of South Africa Limited ("Trust Bank") during September 1972 and, during December 1973, was offered the opportunity to pursue a career in computer technology.
- The expert spent 2½ years in the operational environment with Trust Bank, where he progressed from trainee operator to operations manager. The expert's major functions included shift supervision, daily production and liaison with application development.
- The expert, subsequent to the period spent by him as operations manager, progressed into the field of application development as a trainee programmer with Trust Bank.
- The expert, initially, was trained as a mainframe developer, developing and maintaining banking production systems. During this period the

expert progressed to the position of a systems analyst and became responsible for the quality and standards, as well as technical education, within the Trust Bank's Information Technology ("IT") Division.

- Subsequent to this, the expert became involved in the development and deployment of a leading edge branch banking system which incorporated the electronic transmission of transactions between bank branches and the central computer facility.
- The expert, ultimately in consequence of his exposure to mainframe/work station operating systems, as well as communication networks, became involved in the development of the SASwitch Automatic Teller Machine ("ATM") service and was responsible for the application as well as network level communications systems. Trust Bank, during 1985, became one of the first banks to be an operational SASwitch institution.
- 7 The expert, in time, was promoted to systems adviser within the IT Division at Trust Bank. The expert's responsibilities, as such, included:
  - 7.1 liaison between the IT Division and banking business functions; and
  - 7.2 technical research; and

- 7.3 utilising technology to effectively address business needs; and
- 7.4 providing technical advisory service to critical project development areas; and
- 7.5 keeping senior management abreast of technology developments and trends; and
- 7.6 identifying possible business opportunities as a result of the evaluation of technology; and
- 7.7 developing application integration to hardware based cryptographic platforms; and
- 7.8 developing cross-system and cross-mainframe application interfaces.
- At the time of the absorption of Bankcorp (the holding company of Trust Bank) into ABSA in 1992, the expert had reached the level of senior systems adviser.
- Upon integration of the various personnel groups within ABSA, the expert was assigned to the task team investigating Point Of Sales ("POS") terminal alternatives, as well as possible business avenues in the direction

of "Smart Cards". At this time, First National Bank Limited (as it then was), Nedcor Bank Limited ("Nedcor") and ABSA assigned their respective representatives to a task force to develop standards for a national "Smart Card" system. The expert was the ABSA technical representative, as well as the chairman of the technical sub-committee that set up the standards.

- It was at this time that the expert's specialization in the use of cryptographic hardware and functionality in banking systems, as well as the implementation of holistic security strategies began. The expert was initially assigned the task of establishing an internationally acceptable security standard in ATM and POS applications. This responsibility then grew to include the security requirements of internet based banking interfaces and branch networks, which necessitated self and company sponsored education in the concepts of asymmetric as well as symmetric cryptology.
- By the time the expert terminated his employment with ABSA, he was responsible for the security strategy and architecture for the ABSA Group.

The expert left ABSA in the year 2000 to join Prism Secure Solutions, where his function is to promote and provide cryptographic solutions and products to the banking as well as the retail industry. This entails both internally developed products, and also products provided by

12.

Method rest

Racal/Thales (symmetric cryptology based products) and Baltimore (asymmetric cryptology based products). The latter focused primarily on PKI based implementations. A secondary function of the expert is to provide cryptographic support and consultancy to customer groups that requires such services.

- In summary, the expert has been involved in information technology for the past 27 years and has, for the last 23 years, been directly involved in state of the art banking systems.
- 14 The expert's achievements include the following:
  - 14.1 development of initial IT standards for Trust Bank;
  - 14.2 design and development of an electronic branch processing and transmission system;
  - 14.3 development of an ATM delivery system;
  - 14.4 development of the SASwitch ATM system for Trust Bank;
  - 14.5 development, support and maintenance of encryption techniques;
  - 14.6 liaison with Visa and Mastercard;

4.

- 14.7 rationalisation of Trust Bank/Santam Bank systems;
- 14.8 evaluation and implementation of a POS and ATM Front End System;
- 14.9 home banking investigation utilizing voice biometric systems;
- 14.10 development of inter-region and inter-system application communication systems on IBM mainframes;
- 14.11 development of National "Smart Card" Standards;
- 14.12 development of POS hardware based security modules;
- 14.13 representing ABSA on various technical forums, for example,NPS, SABS, CSIR and COSAB;
- 14.14 branch network hardware based security infrastructure;

1,

- 14.15 centralised security management systems utilizing IBM, DKMS and ICRF;
- 14.16 internet banking security infrastructure utilizing hardware

#### cryptographic engines;

- 14.17 initialisation of the migration to PKI based security;
- 14.18 design, development and implementation of Triple Data Encryption Standard ("TDES") based security systems;
- 14.19 design and implementation of PKI services.

#### Facts of the case

- 15 Mr Anil Singh ("the first defendant") made application on 11 February 1997 for the issue to him of a credit card ("the card") by the plaintiff.
- The first defendant, simultaneously with his application, sought the issue of a so-called additional card ("the additional card") in favour of and for use by Mrs Vanitha Singh ("the second defendant").
- The application was approved by the plaintiff on 24 February 1997 and the card and the additional card were issued by the plaintiff shortly after the approval had been given.
- The card issued to the first defendant bore a card number (which incorporated the account number used by the plaintiff for billing purposes),

viz. 36135828226037 ("the card number").

The card and the additional card were renewed and, more particularly, in respect of the period from December 1999 to January 2001.

who en la service of the service of

On 16 February 2000 the first and second defendants signed application forms utilized by The Standard Bank of South Africa Limited ("SBSA"), it being the issuer of Personal Identification Numbers ("PIN" or "PINs") on behalf of the plaintiff, requesting the issue of PINs for their respective cards.

- Different PINs were issued to the first and second defendants for use by them in conjunction, respectively, with the card and the additional card.

  The PINs were issued out of a so-called 'Auto E Centre' (hereinafter referred to as "the Auto E") owned and operated by SBSA in Chatsworth, Kwa-Zulul Natal.
- The last time that the card and/or the card number was successfully utilised prior to the issue of the PIN associated with the card was on 29 January 2000.
- 23

1.02

Two unsuccessful transactions initiated by the use of the card and its associated PIN were undertaken at two different ATMs owned by Nedcor on 3 March 2000 at 11h26 and at 12h13. The first such ATM was located

at Stanger, Kwa-Zulu Natal and the second such ATM was located at Durban Apartments, Kwa-Zulu Natal.

- The two transactions attempted on 3 March 2000 were for an amount of R100,00 each.
- In consequence of communication received by the plaintiff, the cash facility available to the defendants in pursuance of the use of the card and/or the additional card and the PINs associated therewith was reinstated and again made accessible to the defendants.

26

- During the period Saturday, 4 March 2000, to Sunday, 5 March 2000, a total of 190 successful transactions were effected in consequence of the use of the card, <u>alternatively</u>, a card bearing the card number in association with the corresponding PIN at various ATMs in London, United Kingdom, resulting in a total withdrawal of £54 960,00.
- The withdrawals were effected from ATMs, owned by National Westminster Bank plc, Abbey National plc, HSBC Bank plc and Lloyds TSB Bank plc ("the acquirer banks").
- The first of the ATM transactions in the United Kingdom took place on Saturday, 4 March 2000 at approximately 13h15 and the last ATM transaction, on Sunday, 5 March 2000 at approximately 17h25.

The card and the additional card were returned to the plaintiff's offices in Durban on Monday 6 March 2000, at approximately 17h00.

### Information obtained \_ \\cop \\cop \\

- The plaintiff uses the services of a company called Electronic Data Systems (Pty) Limited ("EDS") to emboss the cards which are to be issued by it to its cardholders.
- The details of the cardholders whose cards are to be embossed by EDS are "captured" on an "embossing tape", which is taken to EDS by the plaintiff's driver either on a daily basis or so often as the needs of approved cardholders might require.
- The tape sent by the plaintiff to EDS contains a so-called Card Verification Value ("CVV") which is created on the IBM 2620 cryptographic processor which the plaintiff has in its premises in Johannesburg, South Africa.
  - The IBM 2620 cryptographic processor is capable of generating both CVV 1 and CVV 2 fields.
- The CVV fields created by the IBM 2620 cryptographic engine contain data of and concerning the Primary Account Number ("PAN"), the service

ě.

code, that is, detail as to where and how the card may be used, and the expiry date of the card. This information, referred to as a cryptographic field, cannot be deciphered, save and except with a cryptographic engine having the identical keys to those used by the plaintiff in its offices in Johannesburg, South Africa.

wind the start

A tape containing the CVV fields and other information necessary for the manufacture of a card is sent to EDS at the end of a "day end process". The "day end" mode or process determines when a tape is created for dispatch to EDS and may or may not result in a tape being created at the end of a particular "day end process", depending on what information is communicated by the computer to the operator regarding the approval of applications.

The system used by the plaintiff can generate cards required urgently, depending on the programming that takes place, that is, the system can be made to perform an additional cycle, under controlled circumstances, such that an additional 'day end process' tape is created containing the necessary information to manufacture such urgent cards.

No PIN generation takes place during the embossing process as the card embossed by EDS contains only CVV 1 and CVV 2 fields, that is, no cryptographic information or data that could be used for purposes of PIN generation or verification.

EDS either sends the cards embossed by it back to the plaintiff for its cardholders to collect at its offices or posts the cards by registered post to its cardholders, depending on whether the prospective cardholder wishes the card to be posted to him or her or has indicated in the application form that the card will be collected by him or her from the plaintiff's offices.

Tapes are sent by the plaintiff to SBSA containing PIN generation requests. A PIN, when used in conjunction with its associated card, enables a cardholder to obtain cash from ATMs worldwide.

SBSA generates a PIN or PINs based on the PIN generation request tape for onward transmission to Diners Club International Service Centre ("DCISC") in the United Kingdom. This enables a cardholder, if he should subsequently wish to use his card and PIN in any place in the world other than the Republic of South Africa and its neighbouring territories (which use the SASwitch system), for example, in the United Kingdom, to access cash at an ATM, the PIN being already extant in an encrypted format on DCISC's computer systems.

The generation of the PIN by SBSA and the despatch thereof in encrypted format to DCISC is entirely independent of any will or wish on the part of a cardholder and takes place on the basis that the mechanisms are in place should they subsequently be required.

<u>,</u>\{;

when control of the state of th

- SBSA does not store any PIN information there is no need for it to do so.
- When SBSA generates the PINs based on the PIN generation request attached to the tape sent to it by the plaintiff, it loads the encrypted PIN numbers created by its computer system onto a different tape which is then sent to the plaintiff the following day. PIN information on the tape sent to the plaintiff by SBSA is conveyed by courier.
  - The tape received by the plaintiff from SBSA containing the encrypted PIN information is read into an AS400 computer at the plaintiff's offices. The information is then passed onto another tape and a control report is ? generated in terms whereof DCISC is requested to run the tape which is to be sent to it by the plaintiff.
- The report is sent by facsimile transmission to DCISC and the hard copy thereof, together with the tape resulting from the processing performed by the plaintiff from the tape received from SBSA containing the encrypted PIN information, is sent to DCISC by courier.
- The information on the tape received by the plaintiff from SBSA is unaltered by it. The plaintiff does not have the keys in its cryptographic γ engine necessary to enable it to decipher the encrypted PIN information

1.

contained on the tape received from SBSA and copied by the plaintiff onto its own tape (being the tape which is subsequently dispatched to DCISC).

- The tape received by the plaintiff from SBSA is then returned to SBSA which deletes the information contained on the tape in order that the tape might then be re-used.
- Every tape used by SBSA and the plaintiff is numbered in order to establish an audit trail.
- A tape generated at the offices of the plaintiff cannot be recreated and the information necessary to generate a tape must accordingly be reprogrammed into the computer and the entire process re-initiated in the event of a card proving, for whatever reason, to be defective.
- The computer system used by SBSA keeps a record of when a PIN request is generated by it and reflects the last request received for a particular cardholder's PIN to be generated and records, *inter alia*, the number of times that a PIN has been issued in relation to a card number.

The tapes sent to DCISC by the plaintiff are sent back to it in batches and are erased by the plaintiff upon their arrival in the Republic of South Africa at its offices.

The account numbers used by the plaintiff have been in existence for a considerable period of time and, in consequence of the number of digits employed by the plaintiff, are re-used from time to time. Once an account is closed, the account number stays on the plaintiff's computer system for approximately two years and if the account is "clean", the account then falls away and the number is then available for re-issue. This means that the same account number may be re-issued after the effluxion of approximately two years and, on this basis, the same PIN number can similarly be re-issued in respect of that account number. All other information, save for the account number, will inevitably be different. The different details associated with the same account number ensure that the correct cardholder is debited in respect of a transaction undertaken by him.

52

1

- The PAN with the exception of the last digit, is used for purposes of generating the PIN.
- A member of the plaintiff wishing to have a PIN issued to him will request SBSA to furnish him with a PIN associated with that member's card number.
- The defendants, in the present instance, requested SBSA's Chatsworth branch that they be issued with their respective PINs which were then issued to them under controlled and managed circumstances. The facility

white of the state of the state

through which the PINs were issued was the Auto E to which reference has previously been made.

The communications technology on which the Auto E operates, in the first instance, is "point to point". It operates, in addition, on a highly sophisticated communications methodology. There are few in the communications industry who have any appreciable understanding of this methodology and they are well known in this industry. The opportunity window for an unauthorised third party to intercept usable information transmitted from "point to point", that is from SBSA's mainframe computer to the Auto E, is so remote as to be discounted.

#### The encryption and usage of "keys"

- The so-called "black box", manufactured by IBM and Thales (formerly Racal) used by the routing and processing participants referred to herein, is a complete cryptographic engine, that is, a computer having an encryption capacity, self protection mechanisms and fitted with a volatile memory.
- The "black box" (also referred to as the hardware security module or "HSM") has a PCB or so-called "green board" which has mounted on it a battery which assures that the volatile memory will hold its state even in the event of there being a loss of external power and, at the same time,

3 (

assures that the volatile memory will be deleted in the event of there being any tampering with the "black box". The "black box" can furthermore be fitted with light detection sensors, movement sensors and access protection switches, all of which are designed to ensure the integrity of the unit in its function as a secure "engine".

- The "black box" is loaded with Local Master Keys ("LMK's"), being so-called "DES" keys that govern all "black box" cryptographic functions. The LMK's are used to encrypt all other DES keys and to encrypt PINs that are to be stored by the host in a database.
- To the extent that the plaintiff and SBSA issue non-random PIN numbers, this results in the same PIN always being derived from the use of, inter alia, the same PAN. Such a PIN is referred to as a "derived PIN" as opposed to a "random PIN".
- When the "black box" is asked to verify a PIN, it responds either positively or negatively. The "black box" does not and cannot be made to respond with "clear data" from "encrypted data" when dealing with information other than PINs. The "black box" will, however, respond with a clear PIN from an encrypted PIN when the required level of authorization has been set as, for example, when a work station operator and supervisor in a bank initiate a secret PIN mailer production.

1.

- The expert knows of no instance whereby a third unauthorized party has been able to access a "black box" (whether by way of a computer programme or otherwise) so as to obtain therefrom the verification of a particular PIN or information regarding the allocation of a PIN to a particular account or for that matter any information contained therein.
- Even if the "black box" were subjected to a physical attack, that is, an assault for purposes of deriving information in an unauthorized fashion, the battery located on the PCB would automatically support the internal firmware in the erasure of the volatile memory and thus renders pointless any further access or tampering. The "black box" is fitted with mechanisms which are designed to ensure its integrity and the integrity of the information stored within it.
- One of the mechanisms or devices which can be used for purposes of securing the environment in which the "black box" is situated is the so-called "sniffer", which is a computer programme designed to identify and warn of any unauthorized electronic attempt at gaining access to the "black box".
- In explanation of the LMK's and their function referred to in paragraph 59 above, the following facts are relevant:

Ť.

65.1 three "components" (either a 16 or 32 character long random

hexadecimal number, depending on the institution in question either using single or double length keys, each such component being the same length as the resultant key) are either randomly generated by computer or decided upon by individuals to whom the task is allocated:

- the creation of the components takes place in a manner which ensures that the components can never be brought together save and except within the controlled environment associated with the "black box" in question;
- 65.3 the components are loaded into the "black box" in an environment which ensures the secrecy of the components and the "black box", upon having the components loaded into it, then, by a mathematical process generates the LMKs or base keys;
- the LMKs thus generated are specific and peculiar to the cryptographic engine or engines (as the case might be) used by the institution in question;
- the LMKs are used only to create variants of themselves which, in turn, are then used for specific tasks;
- 65.6 the variants always operate in pairs, that is, there will always be

Í.

two keys "created" for a specific application;

- of variants created from LMKs are used to verify or create data from input parameters;
- once the variants have been created, the application driving the "black box" can issue an instruction to create the PIN Master Key ("PMK");
- the function of the PMK is PIN verification and PIN generation;
- the "black box", in generating the PMK, generates 16 random hexadecimal digits (also referred to as either a 64 or 56 bit number) which is the PMK in the clear (within the "black box");
- the "black box" selects the relevant pair of LMK variants to apply TDES to the 16 hexadecimal digit number, which results in an encrypted PMK;
- the encrypted PMK is then given to the host programme at SBSA (for storage).

66

1,

66.1 Insofar as the creation or generation of the Zone Master Key

("ZMK") is concerned, the loading of three similar components referred to in paragraph 63.1 above takes place in exactly the same fashion as was the case for purposes of the creation of the LMK. The three components were sent separately and individually to SBSA by DCISC and are the same components used by DCISC for purposes of creation of the encrypted ZMK at DCISC.

- The ZMK (which cannot be created at all unless the "black box" is "loaded" with LMKs) is loaded at both SBSA and DCISC encrypted under their respective LMKs.
- The consequence of the aforegoing is that both SBSA and DCISC have the same ZMK, whilst SBSA, in addition, would also have the PMK which DCISC would not be allowed to have.
- SBSA, by virtue of it having the ZMK, is in a position to encrypt a PIN for transportation to DCISC.
- The stored ZMK is encrypted (on the DCISC database) under variants of the DCISC (not SBSA) LMKs.
- Upon receipt of the file of encrypted PINs and associated information from the plaintiff, the following occurs at DCISC:

1.

- a record of cardholder details is electronically read and the ZMK encrypted PIN is extracted;
- the LMK encrypted ZMK and the ZMK encrypted PIN are passed to the "black box" for translation (of the PIN) to another variant of the LMK;
- 67.3 the "black box" decrypts the ZMK using the LMK variants, which is then in the clear but inside the "black box" (that is, not visible);
- the decrypted ZMK is then used by the "black box" to decrypt the
  PIN, which is then in the clear but, once again, inside the "black
- the PIN in the clear (inside the "black box") is then encrypted by a variant set of the LMKs in TDES format and stored for future access/verification purposes.
- DCISC has a zone-based relationship with, for example, a switch institution such as Transaction Network Services (UK) Limited ("TNS"), as it is now known, which means that TNS will have a ZMK which is common to the ZMK which the Card Authorisation Front End System ("CAFES"), which is managed by DCISC, has (but not common with any other set of

\*.

ZMKs in any other zone).

- Each entity in the routing has a zone-based relationship with the next entity in the routing and it is through the ZMK that the entities are able to exchange Issuer Working Keys ("IWK's") and Acquirer Working Keys ("AWK's") which are Session Keys ("SK's), which enable the onward translation and transmission of encrypted PIN blocks to ultimately get to the verification point (in the present case, the RELAY system utilized by DCISC).
- The use of a card bearing the card number and PIN as aforesaid gives rise to data which is electronically transmitted from the ATM in question to:
  - 70.1 the acquirer institution from where it is then transmitted to
  - 70.2 Link Interchange Network Limited ("LINK") which, like TNS, is a switch from where it is then transmitted to
  - 70.3 TNS which, as aforesaid, is a further switch from where it is ultimately transmitted to
  - 70.4 DCISC's computer systems.

10

71 TNS, being one of the two switch entities (the other preceding switch

being LINK) "sees" DCISC's systems as the issuer of any Diners Club card that is performing the transaction. LINK and TNS look at the PAN in the information received by them and are able to establish that such a card is a Diners Club card.

AWK to the "downstream" IWK and ultimately transmit the information "downstream" to the RELAY system at DCISC.

73

- 73.1 The switch entities, in the aforegoing process take, from their own database, the following :
  - 73.1.1 in the case of LINK, the AWK of, for example, one of the acquirer banks encrypted under the relevant variants of the LMK; and
  - in the case of TNS, the IWK of CAFES which is also encrypted under the same variant of the LMK and translates the AWK encrypted PIN block to IWK encryption for forwarding to CAFES.
- The assumption is made that the ATM, host bank, switch entity and DCISC all use ISO 0 for purposes of PIN block formatting.

74 The transaction, upon its arrival at the RELAY system used by DCISC. requires verification. The data elements which are passed on to the "black box" for verification comprise: 74.1 the IWK encrypted under the LMK variant set; 74.2 the PAN; 74.3 the PIN block which is IWK encrypted; 74.4 the PIN which is LMK variant set encrypted. 75 The "black box", upon receipt of the fields as set out in paragraph 74 above, then: 75.1 decrypts the IWK; 75.2 decrypts the PIN block with the clear IWK; reverses the XORing process performed on the PIN; 75.3

decrypts the PIN with the LMK variants;

75.4

- extracts the PIN from the PIN block because it (the "black box")

  "knows" the position of the PIN in the PIN block and compares
  the incoming PIN with the PIN that was previously stored under
  the LMK variants.
- The rule which is employed between a bank (in this instance DCISC) and a switch entity is that when the communication session between their respective computer systems commences, they will move to a mode which causes the establishment of SKs (that is, IWK and AWK) prior to any transactions being permitted.
- The storage of the encrypted PIN is secure because the encrypting keys reside within the "black box", which is access controlled, and because of the encryption process used.
- The "route" that is followed when a "black box" communicates to another, is referred to as a "zone".
- Information transmitted in a zone, insofar as a PIN is concerned, will always be encrypted and it is only when a PIN is issued to the plaintiff's cardholder, that is, that the information is not being passed on within a zone, that the PIN occurs in the clear. Even when the PIN is to be stored in a database, the PIN exists in an encrypted format.

`

- The combination of the information contained in the so-called "mag strip" encoded on the back of a card issued to a cardholder of the plaintiff and the PIN enables such a cardholder to obtain cash from an ATM.
- An ATM will not dispense cash unless both the plastic card containing the mag strip and the PIN associated with or linked to the information contained in the mag strip are presented to the ATM as part of one and the same transaction.
- The information keyed into an ATM by the user, that is, the PIN, is captured by a cryptographic engine incorporated in the keypad.
- The keypad on the ATM, in effect, constitutes or comprises an integral part of the cryptographic engine or HSM or Tamper Resistant Security Module ("TRSM") or "black box".
- The act of inputting the PIN into the keypad which has incorporated in it an HSM, results in that information, that is, the PIN being immediately encrypted using the Terminal PIN Key ("TPK") programmed into the HSM/keypad.
- Once encrypted, the encrypted PIN number, formatted according to one of the recognized PIN Block formats (e.g. ISO 0), is then transmitted from the ATM to the acquirer bank (that is, the bank owning the ATM), which has

its own HSM into which the same TPK has been loaded.

The electronic transmission of the encrypted PIN Block from the ATM to the acquirer bank follows a route (as aforesaid), which is referred to as a zone.

The acquirer bank's HSM has loaded into it not only the working key located in the ATM, but other working keys which enable the encrypted message to be translated and transmitted (again electronically) from the acquirer bank to another institution, that is, in the present instance, LINK which, in its turn, translates and routes the encrypted message "downstream" ultimately to the RELAY system at DCISC.

88

\*

In the event of the card in question belonging to the acquirer bank, the switch institution will have no role to play in the transaction and the information will simply pass between the ATM and the acquirer bank and, depending on the location of the ATM, between the branch of the acquirer bank in question and the host of the same bank. The switch institution, in such circumstances, would have no role to play in the transaction.

To the extent, however, that a switch institution becomes involved in the transaction, it, in turn, enjoys a multiplicity of keys, one of which would be the same AWK as that held by the acquirer bank, which would then enable the switch institution to receive the encrypted information, which

would then be translated into a different working key, that is, the IWK, which correlates precisely with an IWK stored in the HSM of the RELAY system at DCISC.

Simultaneously with the transmission of the encrypted PIN Block from the ATM to the acquirer bank to the switch institution and ultimately to the RELAY system at DCISC, the information contained in the magnetic strip is transmitted, via the same route, to the RELAY system and, for reasons which are hereinafter set forth, and most importantly, via LINK, TNS and CAFES.

The transaction data generated by the ATM itself is transmitted together with the encrypted PIN Block and the magnetic strip data and it is this which serves to produce a record of the transaction, excluding the encrypted PIN Block.

The intervention of a switch institution in circumstances where the card used at the ATM has been issued by an institution other than the acquirer bank, is seminal to the identification of the destination to which, *inter alia*, the encrypted PIN Block information is to go. The first six digits (and sometimes the first eight) of the card number, when received by the switch institution, dictate the identity of the ultimate recipient of all of the aforegoing information. Insofar as there exists a contractual relationship between the plaintiff and SBSA, the verification of transactions originating

from the usage of a card issued by or on behalf of the plaintiff will, should the transaction have occurred within the geographical SASwitch "arena", result in the transaction being routed to SBSA for verification. To the extent, however, that the transaction takes place outside of the SASwitch "arena", the transaction is then routed to DCISC for verification.

In order for LINK to be able to direct the information transmitted to it, the HSM which it maintains is programmed, amongst other things, with the working key used by the acquirer bank, that is, the SK. The HSM used by TNS, in its turn, is programmed with the SK for receipt of the transaction information from LINK and a different SK for transmission of such information to CAFES.

The only information that is transmitted from an ATM to an acquirer bank or a switch institution or an issuer (as the case might be) in an encrypted form is the PIN Block. All other information generated by the use of a card and PIN (that is, the information subsumed in the magnetic strip and the transaction data generated by the ATM itself) is transmitted in clear form.

Provided that the information received by the RELAY system is reconcilable with its database, that is, that the encrypted PIN information correlates with the account details pertaining to the same PIN, the transaction is authorized on behalf of the plaintiff. In the event that the plaintiff has imposed an authorization limit and the transaction amount is

below that limit, the transaction would not require any further authorisation.

- To the extent that there is no separate requirement for authorisation, the RELAY system would simply transmit an advice of the transaction to the plaintiff for its records.
- The ultimate purpose and objective of encryption is to achieve a safe and/or secure means of transmitting information which, by its nature, is highly confidential and privy to the client/cardholder. Encryption serves to protect both the cardholder's interests and also those of the issuing bank (and, for that matter, all of the institutions involved in the transaction routing) as the case might be.
- The plaintiff, insofar, inter alia, as personal cards are concerned, is able to generate what might be called an "ATM negative file" in respect of cardholders for whom cash will not be made available and also for purposes of establishing a limit to the amount of cash which those who can have access to cash from an ATM would be allowed to obtain.

## THE OPERATION OF AN ATM AND, MORE PARTICULARLY, A NEDCOR ATM IN THE REPUBLIC OF SOUTH AFRICA

The expert will further give evidence that:

99

t.

- the information keyed into the ATM by the user, that is, the PIN number, is captured by a cryptographic engine incorporated in the keypad of the ATM; and
- the keypad on the ATM, in effect, is an integral part of the crypto engine or HSM (also referred to as a TRSM or "black box"); and
- the act of keying in a PIN into the keypad which forms part of the cryptographic engine results in the information keyed in, that is, the PIN (in the clear) being immediately encrypted using the Terminal PIN Key ("TPK") programmed into the HSM/PIN pad. This means, the expert will testify, that the PIN is never transmitted in the clear; and
- once encrypted, the encrypted PIN number, formatted according to one of the recognized ISO PIN block formats, is then transmitted from the ATM to the host bank which owns an HSM into which the same TPK has been loaded; and
- the electronic transmission of the encrypted PIN block from the ATM to the bank follows a pathway (as aforesaid), which is referred to as a zone; and

4.

- so the host bank's HSM has loaded into it not only the working key located in the ATM, but other working keys which enable the encrypted message to be translated and transmitted, electronically, from the bank to SASwitch, which switches the particular transaction; and
- 99.7 the electronic process whereby the encryption of a PIN keyed into an ATM is ultimately identified by the issuer bank, is not susceptible either to malfunction or to unauthorized intervention by or on behalf of a third party.

#### 100 The witness has been advised that:

- the first defendant, during the afternoon of 3 March 2000, telephoned the offices of the plaintiff in Johannesburg in order to advise the representative of the plaintiff to whom he spoke that he had attempted, on two occasions, to use the card and the PIN allocated in respect thereof for purposes of withdrawing cash from two different Nedcor owned ATMs and that both such transactions had been declined; and
- the first defendant further advised the plaintiff's aforesaid representative that he (the first defendant) was "... not prepared to wait till Monday for PAYM (sic) to be allocated (the plaintiff)

made error (sic) & (the plaintiff) ... must allocate today ..."; and

the first defendant had made payment to the plaintiff which had been misallocated and which, upon receipt of the first defendant's telephone call, was re-directed to the correct account number so as to remove the defendants' account from the negative file to which it had been allocated, resulting in the defendants' account enjoying a status which would entitle the defendants, upon use of the cards and PINs allocated to them, to withdraw cash from an ATM; and

another representative of the plaintiff (different to the first mentioned) spoke to the first defendant on 3 March 2000 in order to advise him that the plaintiff "... will sort (it) out & he dont (sic) want to draw cash (he) was worried that he is going Monday to India & he will pick up problems ... (the plaintiff's representative) told him (that it) will be sorted (out) ..."; and

the removal of the defendants' account from the negative file and the establishment of the account as being "live" in the plaintiff's systems was effected on the same day, that is, 3 March 2000.

The expert has been advised that had any malfunction of the ATMs owned by Nedcor and installed at Nedbank Stanger, cnr Hulett and

Jackson Streets, Stanger, having identifier number K725 and at Durban International Airport, Domestic Arrivals, Isipingo, having identifier number L234 taken place on 3 March 2000, it would have been identified by SBSA and that the records reflecting the attempted withdrawal of funds from those ATMs by the first defendant or authorized by him, show that the said ATMs were functioning properly.

- The expert, based on the aforegoing, and given his experience with the operation of SASwitch, a switch operated by a consortium of the major South African banks and performing the same function as LINK and TNS, makes the following points and/or observations regarding the use by the first defendant of the card and its associated PIN at a Nedcor owned ATM on 3 March 2000. Thus:
  - the use of the card and its associated PIN at a Nedcor ATM would have resulted, *inter alia*, in the encryption of the PIN in consequence of the keying in of the PIN on the ATM's keypad; and
  - the encrypted PIN, together with the other information generated in consequence of the insertion of the card bearing the magnetic strip and the instructions keyed in by the first defendant, would have been transmitted, electronically, to Nedcor's mainframe computers which, upon receipt of the information, would have

recognized the encrypted PIN as belonging to an institution other than Nedcor. Nedcor's mainframe computers would then immediately, the PIN having been decrypted and re-encrypted in an HSM, have forwarded the information (including the encrypted PIN) to SASwitch. SASwitch, in its turn, would, having first decrypted and re-encrypted the PIN in its HSM, have electronically transmitted the data to the banking institution that its computer systems would have recognized as being the issuing bank; and

- the issuing bank, insofar as cards issued by the plaintiff are concerned, as aforesaid, is SBSA, which ultimately, through its computer systems, would have been in a position to recognize the PIN and either authorize or decline the transaction, as the case might be; and
- the rejection of the transactions attempted by the first defendant on 3 March 2000 would have come about in consequence of SBSA's computers having been alerted to the negative status of the defendants' account, such status being communicated to it on a daily basis by the plaintiff by way of a tape created by the AS 400 computer used by the plaintiff and the transportation of such tape from the plaintiff's premises to the premises used by SBSA for purposes of housing its mainframe computers.

# THE OPERATION OF THE ATM INDUSTRY IN THE UNITED KINGDOM

- 103 The expert has had the opportunity to consult with:
  - 103.1 Mr Alexander Leckenby ("Leckenby"), the security administrator of LINK; and
  - 103.2 Mr Adrian Walker ("Walker"), the manager of the technical support team of CAFES; and
  - Mr Michael Bird ("Bird"), the development manager for the RELAY and INTERCHANGE systems used by DCISC for purposes of processing, *inter alia*, transactions resulting from the use of cards issued by the plaintiff; and
  - Mr Allen Mortlock ("Mortlock"), the person responsible for the business interface between the technical groups (Cardholder And Merchant Processing Systems ("CHAMPS") and CAFES) and Diners Club International franchisees.
- The expert, in consequence of his discussions with Leckenby, has apprised himself of the manner in which an encrypted PIN is dealt with by LINK, from the time that the electronic data stream reaches the computer

4

systems utilized by LINK to the time that the encrypted PIN is electronically transmitted onwards by the said computer systems and has satisfied himself that the processes employed by LINK ensure the integrity of the transaction as a whole and of the PIN itself and comply with the standards laid down by the International Standards Organisation ("ISO").

- The expert is furthermore satisfied that the manner in which the encrypted PIN is dealt with by LINK does not admit of any failure of the system or of any unauthorized third party intervention.
- The expert is of the same views insofar as the systems operated by DCISC are concerned and, in this regard, has satisfied himself that CAFES, CHAMPS, RELAY and INTERCHANGE are all similarly not susceptible to failure or to unauthorized intervention by a third party and comply with the standards laid down by ISO.
- The expert, as is apparent from the reasons expressed by him hereinafter, does not consider it possible that any of the systems employed by DCISC could have "made a mistake" in allocating debits which ought to have been ascribed to a hypothetical "Mr A.N. Other" to the defendants' account or that the systems could have malfunctioned so as to generate fictitious transactions or that there could have been any extraneous injection of false or counterfeit information.

To the extent that a duplication of 35 transactions allocated by the plaintiff to the defendants has occurred, the expert is satisfied that the duplication arose in consequence of a human error and not an electronic or mechanical error. The information that was duplicated was correct: the mistake lay in the instruction given to the system which brought about the duplication. The duplication related only to the systems' billing functions and not to the authorisation or verification processes.

The expert has had an opportunity to read the notices in terms of Rule 36(9)(a) and (b) to be delivered on behalf of the plaintiff in respect of the testimony of Leckenby, Walker, Bird and Mortlock and is satisfied that the summaries constitute a correct rendition of the information given to him by the parties in question during the course of his consultations with them as aforesaid and that the summaries support the views expressed by him herein.

### THE EXPERT'S OPINIONS AND REASONS THEREFOR

110

4

## 110.1 The first opinion

The expert is of the opinion that the "black box" is tamper proof (hence it being referred to as a Tamper Resistant Security Module or TRSM), and, as such, impervious to any access or

intrusion, save and except for that expressly and specifically programmed.

### 110.2 The expert's reasons for the first opinion

DV 7

The "black box" is fitted with motion, light and/or access detectors which, if disturbed, trigger the firmware referred to in paragraph 58 above, which, as previously indicated, will erase the volatile memory independently of any other power source (as the unit has an internal battery/power source) that may or may not be connected to the "black box". Anything stored in the memory, for example, the LMKs or DES keys, will be automatically erased, leaving no trace in the "black box". By the same token, any encrypted or clear PIN existing in the "black box" at the time that any tampering takes place will be deleted therefrom. The only basis upon which a four digit PIN could be extracted from the "black box" would be for a so-called "brute force" attack, which requires the application of a computer programme designed to input multiple permutations of the four digit PIN (there being a potential of 10 000 such permutations) in the hope that the PIN number will be indicated by the "black box" to be correct at some stage prior to the input of the 10 000th permutation. introduction of such a programme into any part of the circuitry associated with the "black box" would constitute an unauthorized

application and would result in the 'sniffer', referred to in paragraph 64 above, disconnecting the "black box" from the computer network, thereby forcing the attack to be discontinued. The "black box", on this basis, is impenetrable.

111

### 111.1 The second opinion

The initial generation of the PIN is safe and secure.

# 111.2 The expert's reasons for the second opinion

The process of PIN generation takes place within highly secure object code. The source code to the object code is not available to SBSA. As a result of this, SBSA cannot apply any changes, legal or illegal, to the object code. Access to and use of this object code is protected by "TOP SECRET", a computer access and authorization control system.

112

1

### 112.1 The third opinion

Even if the zone and therefore the encrypted PINs were violated, the information would be of no value.

## 112.2 The expert's reasons for the third opinion

Firstly, it is in any event unlikely that the zone would be violated because of the prohibitive cost and time involved in attempting to do so. Secondly, even if the encrypted PIN were to be violated, it would be of no value without the track 2 card information.

113

## 113.1 The fourth opinion

Notwithstanding that a four digit PIN results in there being a finite number of permutations, that is, 10 000 and that, as a consequence, there will be cardholders of the plaintiff who will have the same PIN number, this does not compromise or otherwise detract from the integrity of the card system implemented and employed by the plaintiff.

### 113.2 The expert's reasons for the fourth opinion

The PIN number issued by SBSA on behalf of the plaintiff, as referred to in paragraph 60 above, is a derived PIN as opposed to a random PIN. A derived PIN arises in circumstances where the account number allocated to a cardholder of the plaintiff will

1.

dictate the permutation of the PIN and ensure that the same PIN number is generated everytime the PMK generates a PIN in respect of the specific account number. The reason for this is that all PINs generated by SBSA on behalf of Diners Club are socalled "system generated PINs", the cardholders of the plaintiff not being able, given the manner in which the system is operated, to select their own PIN numbers or change the PIN number allocated to them by the system. System generated PINs are created using an encryption key, a standard algorithm, the card number and a decimalization table used to transform the PIN number to numeric form (from hexadecimal form). encryption key used is the PMK. The first four digits of the generated number are then used as the PIN. Due to the static values that are input into this process, the PIN will always be the same for a particular card number. The "marriage" between the PIN and the card number will always be unique to the specific card number. Given that PIN Block format ISO 0 is used in the PIN verification process, there will, on this basis, be no scope for or possibility of two cardholders of the plaintiff having the same PIN number having their transactions confused one with the other. The "marriage" will ensure that the transactions pertaining to a specific card number, notwithstanding that the PIN associated therewith might be the same as another PIN issued on behalf of the plaintiff, are correctly debited and allocated as

against the account which correctly and legitimately falls to be debited.

114

### 114.1 The fifth opinion

The PIN cannot be gleaned from the magnetic strip installed on the reverse of a credit card.

### 114.2 The expert's reasons for the fifth opinion

The magnetic strip which is embedded in the plastic constituting the credit card does not contain information which would yield, whether by the application of a crypto engine or otherwise, the detail of a PIN. This is as a result of there being no cryptographic value, typically a PIN Verification Value ("PVV") associated with the actual PIN, encoded on the magnetic strip on the back of the card.

115

### 115.1 The sixth opinion

An attempt to obtain a PIN by a process of trial and error, that is, multiple attempts, at an ATM would not succeed.

#### 115.2 The expert's reasons for the sixth opinion

ATM's, worldwide, are programmed, after, in some instances, the third attempt and, in other instances, the fifth attempt, either to "absorb" the card used for purposes of the transaction, that is, to retain the card and not release it to the user of the machine or to reject the transaction and return the card to the card-holder on one basis or another, based on an instruction issued by the 'issuer institution', in this case being DCISC. The "PIN re-try" management adopted by financial institutions owning ATMs is such that multiple attempts at obtaining the correct PIN for purposes of the transaction are precluded.

116

#### 116.1 The seventh opinion

The integrity of the PIN management in the transaction cycle ensures that there can be no third party interference with or access to the PIN during such cycle.

### 116.2 The expert's reasons for the seventh opinion

The encryption of the PIN at the time of use ensures that the

ţ.

detail or data pertaining to a particular PIN remains inviolate throughout the life of the PIN.

117

#### 117.1 The eighth opinion

There is no margin for error in the allocation of debits during the on-line transaction processing.

### 117.2 The expert's reasons for the eighth opinion

The combination of information subsumed within the PAN read in conjunction with the PIN Block makes it impossible for there to be an electronic error in the allocation of a particular transaction as against a particular account. Even if two cardholders should have the same account number and the same PIN number, this will not result in the transaction amount being incorrectly debited, as the only basis upon which this could transpire would be that the account number and the associated PIN had been deleted from the plaintiff's system prior to them being re-allocated. By the same token, the information encoded on the magnetic strip (including the expiry date of the card) would ensure that there is no margin for error insofar as the accounting pertaining to a particular transaction is concerned.

į.

118

## 118.1 The ninth opinion

An ATM transaction is not feasible without both a card whose magnetic strip carries the authentic information and the derived PIN being present at the ATM simultaneously.

### 118.2 The expert's reasons for the ninth opinion

The reasons for the aforegoing opinion arise in consequence of the reasons already set forth above.

119

1

### 119.1 The tenth opinion

It is almost impossible that the information on the magnetic strip on the plaintiff's card and the PIN could have been obtained by a third party without the plaintiff having given the PIN and card to such third party.

### 119.2 The expert's reasons for the tenth opinion

119.2.1 Whilst it is not impossible to install a "sniffer" on a

system and decrypt the information, the process is time consuming and very costly (the machinery necessary to perform the exercise costing not less than R200 000,00).

119.2.2 The expert knows of no occasion which has been reported either in South Africa or abroad where the PIN has been obtained in this fashion and the probability of this occurring in relation to a single card is so remote as to be discounted.

119.2.3 The Nedcor and SBSA systems were not violated or tampered with.

119.2.4 Even if the magnetic information on a card is copied, it is worthless for ATM transactions without the corresponding PIN and vice versa.

119.2.5 The PIN, both in storage and whilst being translated, is inviolate.