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

	Case No: 00/3156
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 MICHELLE ERIKSEN

**TAKE NOTICE** that Michele Eriksen will, at the hearing of the trial of this matter, give expert evidence on behalf of the Plaintiff as hereinafter set forth.

1. The curriculum vitae of the witness is annexed hereto marked "ME1".

- 2. The witness is presently the Network Security and Encryption Service Manager of the Standard Bank of SA Limited ("SBSA") and in such capacity is in charge of the encryption programmes which she took over in 1996.
- 3. Part of the system taken over by her was the Plaintiff's PIN master key.

  The witness wrote new systems and has particularly been engaged in converting the SBSA system to the new "Black Box" model i.e. from the IBM 4753 to the Integrated Cryptographic Resource Facility.

The witness has been advised that:

ţ.

- 4.1. during or about 1993 Diners Club SA (Pty) Limited, the Plaintiff, implemented a system of personal identity numbers ("PINS") for use with the cards issued by the Plaintiff to its cardholders;
- 4.2. generation of PINS was implemented on the SBSA infrastructure, that is, on the mainframe computer utilised by SBSA for purposes of generating PINS for its customers;
- 4.3. Diners Club International Service Centre ("DCISC"), based in the United Kingdom, created three component parts which, when added together, made up the master encryption key;

- 4.4. the three components were sent by DCISC to the Plaintiff separately and, more particularly, to three representatives of the Plaintiff;
- 4.5. The aforesaid representatives upon receipt by each of them of the respective component of the encryption master key, in a secure manner, entered the components allocated to each of them into the SBSA mainframe computer;
- 4.6. the PINS generated by the SBSA mainframe computer were (and are) not issued to the card member automatically and were (and are) issued only upon application therefore;
- 4.7. Plaintiff, upon receipt of an application for membership and such application being approved, furnishes SBSA with a tape recording the information pertaining to such card holders including, *inter alia*, the account numbers allocated to each such card holder;
- 4.8. the SBSA mainframe generates PINS using the PIN master key ("PMK") in respect of each of the cardholders whose information has been captured on the tape. In order to do this the tape which is delivered by the Plaintiff to SBSA is loaded onto the SBSA computers and at a predesignated time the encrypted PIN in relation to each new cardholder is then

recorded on a tape and the two tapes are returned by SBSA to the Plaintiff:

- 4.9. upon receipt by the Plaintiff of the tape by SBSA, the tape which initiated the process is recycled whilst the tape containing the encrypted PINS is read into the Plaintiff's IBM AS400 computer for purposes of reformatting, resulting in the creation of a new output tape. The new tape thus created is sent by courier to DCISC in the United Kingdom with a control report which is also sent to DCISC by facsimile transmission;
- 4.10. the encrypted PINS are stored off site in order that the use by a cardholder of Plaintiff of his card and PIN in a network other than one covered by SASwitch or SBSA might be verified.
- 5. Based upon the aforegoing and such additional data and reasons as appear hereinafter, the witness will give evidence that:
  - 5.1. The principles of good Key Management were implemented and followed by SBSA in generating PINS on behalf of the Plaintiff;
  - 5.2. The operation of the mainframe computer has changed since 1993. In 1993 SBSA were making use of software Crypto (PCF). Later SBSA implemented hardware Crypto (4753). As

far as this concerns the Plaintiff, PCF was used until 2000 for the generation of the PIN for the tape, however, the PIN validation process for Plaintiff through SASwitch and the PIN issue through the branches makes use of the 4753;

- 5.3. The mainframe computer of SBSA, in simple terms, is linked to a keyboard and it is via the keyboard that the three component parts making up the encryption key were loaded into the mainframe and, in turn, passed to the IBM accredited Cryptographic Functionality i.e. PCF;
- 5.4. The components, whilst they are in the PCF domain, are combined to produce an encryption key which encrypts all PINS which are subsequently issued in clear form to a cardholder of Plaintiff upon request. The encryption key is then encrypted by the relevant pair of local master keys for output and storage to a key management file. Access to this file is controlled so as to ensure that only authorised persons or applications can read or update it;
- 5.5. The SBSA mainframe, using the encryption key, that is, that Zone Master Key ("ZMK") shared with the Plaintiff encrypts the PINS;

5.6.

The key (PMK) used by SBSA for purposes of generating PINS on behalf of Plaintiff is not the same key as that which is used to encrypt the PIN when stored in the computer at Meerbusch in Germany and which is used for purposes of verification of a PIN used in a transaction in a country not linked to the SASwitch network;

5.7. The PMK, Prime Account Number ("PAN"), decimalisation table, PIN block encrypted under the IWK and the IWK encrypted under the Local Master Key ("LMK") variant (this information being referred to as "fields") is passed from the SBSA mainframe to the IBM 4753 HSM or "Black Box". The PAN, decimalisation table and PMK (encrypted under the LMK variant) are used to derive the original PIN for the cardholder:

- 5.8. For the purposes of verification the PIN block is decrypted using the IWK to expose the clear PIN therein and the original PIN and the clear PIN thus disclosed are then compared for conformity;
- 5.9. All the PIN processing is performed within the confines of the "Black Box" which is a secure and tamper resistant environment;

\* .

- 5.10. The management of keys and PIN issues is governed by the standards issued by the International Standards Organisation ("ISO") as well as the regulations and requirements specified by VISA and Mastercard;
- 5.11. SBSA uses two systems for the provision of PINS namely the BDS, at the branches, and the direct transmission to the Micro-Swop systems resident in the Auto-E Centres from the mainframe. In relation to the latter the PIN is transmitted in the "clear" whereas in relation to the BDS machines the transmission is encrypted;
- 5.12. Notwithstanding the fact that, under the older machines, the PINS are, in the process of issue, transported in the "clear," the PIN generation by SBSA in this fashion has not, to the witnesses' knowledge, during the period from when she took over the programming in 1996 to date, been violated in the sense that any third party has accessed the transmission and obtained the "clear" PINS being so transmitted;
- The transmission of PINS under the BDS process is secure and similarly there has been no violation of that system whilst it has been operated by SBSA.

- 6. In relation to the action between the Plaintiff and the Defendants the witness has been informed that:
  - 6.1. the application for the issue of the Diners Club credit cards was made on the 11<sup>th</sup> February 1997 and approved on the 24<sup>th</sup> February 1997;
  - 6.2. on the 16<sup>th</sup> February 2000 the Defendants made application for the issue of PINS in relation to their respective cards;
  - 6.3. other than two failed transactions on the 3<sup>rd</sup> March 2000, neither of the Defendants' Diners Club cards and associated PINS were utilised by the Defendants until the 4<sup>th</sup> March 2000;
  - 6.4. 199 transactions, 190 of which were successful, took place during the 4<sup>th</sup> and 5<sup>th</sup> March 2000 in consequence of the use of card number 36135828226037 which was issued to the First Defendant;
    - 6.5. the First Defendant has denied that the ATM transactions were transacted by him or the Second Defendant and contends that, at the time of the transactions, they were not in London, where they were transacted, the Diners Club card had not been given to anybody and the associated PIN had not been revealed to anybody.

- 7. Insofar as it might be suggested that a third party was able to access the SBSA system for the generation of the PINS to the Defendants prior to or at the time of the issue of such PINS to them, the witness, based on the aforegoing, will give evidence that:
  - 7.1. there was no attempt to tamper with the SBSA Cryptographic platform ("Black Box");
  - 7.2. no unauthorised party gained access to the SBSA system for the generation and communication of PINS;
  - 7.3. consequently, if any access to the "clear" PIN was divulged to any third party, it could not have taken place before or simultaneously with the PIN being delivered to the Defendants;
  - 7.4. there was no misallocation of the PINS to the respective cards.

1.

### CURRICULUM VITAE of

#### Michele Eriksen

ANNEXURE "ME.1"

#### **SUMMARY**

Eleven years experience in the information processing industry including information analysis, system design, programming, procedure development, implementation, performance monitoring and tuning, conversion, maintenance, support and training. Eight years experience in the Information Security area, including network and Internet security and encryption, including implementation and key management.

Over 14 years experience in the use of PC's and PC packages.

Ability to communicate effectively at all technical, operational and administrative levels.

Wide range of experience in applications, software and hardware.

#### **Applications:**

Encryption in various environments Information Security Network Security Internet Security Product Accounting

#### Software:

#### Mainframe

**IBM Encryption Interfaces** 

CICS, Cobol

Easytrieve

TSO/ISPF

OS/390

**REXX** 

Clist

Top Secret

**IBM Transaction Security Services** 

PC's

Access, Excel, Word, Powerpoint

Wordperfect

Lotus 123

Lotus Freelancer

**IBM Transaction Security Services** 

#### Systems:

MVS/ESA & MVS/XA

Windows

OS/2

DOS

#### Hardware:

IBM 9221, 3090

IBM PC's

Compaq PC's

IBM 4753, 4755, 4758 & ICRF HSM's

NCipher Encryption Units

**Racal Encryption Units** 

#### **DETAIL**

4

#### 8/92 - Current Standard Bank of SA, South Africa

Manager, Network Security and Encryption Services

Currently managing nine staff members who are required to provide expert advice and counsel to both Management and Technical personnel on all aspects of information, protection, with specific reference to those applications for which encryption methodology and security over the networks is required. In addition, there is a requirement to initiate and provide the technical direction for the information security platform, by designing the security infrastructures and implementing new levels of software and techniques, in order to meet stringent information security criteria across the group. Also required to add value by supporting the Group's strategic initiatives across all technology platforms through the design, development, implementation, maintenance, communication and coordination of policies and standards for information protection.

Responsible for the continued maintenance of all encryption code for the OS/390 and MVS environments.

#### Duties include:

- Aid the career development of subordinates through the allocation of tasks, on-the-job instruction, conducting formal/informal performance appraisals and constructive critical supervision, which will ensure effective job succession opportunities.
- Maintain written job descriptions for subordinates and actively promote and support the Group Policies and targets for Employee diversity.
- Ensure Information Security Analysts are adequately trained and equipped to protect the Group's Information assets.
- Analyse and evaluate the management of risk in terms of Information Security, with particular emphasis on the Encryption methodology and Network Security, and proactively implement appropriate compensating controls.
- Develop, publish and monitor the implementation of Information Security Policies and Standards to ensure that loss of data integrity or confidentiality or fraudulent manipulation of data is effectively contained.
- Ensure the cost-effective application of security techniques such that computer processing performance and throughput is not adversely affected, without compromising the desired level of information security.
- Provide a Group wide information security consulting service to those entities whose computer operations are independent of ISD Control.
- Provide technical guidance for the implementation of Information Security requirements to the Information Security Analysts and other IT and Business personnel.
- Provide statistical information on security related incidents to senior management, develop and implement control procedures to eliminate redundancy of security definitions
- Administrative tasks: provide statistical information, limited customer support, cleanup tasks. Document standards and procedures with regard to the different security platforms supported by the department.
- Monitor the performance of suppliers so as to ensure that they meet their service level
  obligations. Meet with existing and potential suppliers regularly in order to be informed
  on new products / techniques which could be used to improve the levels of information
  security.

# CURRICULUM VITAE of Michele Eriksen

ANNEXURE "ME.1"

• Ensure the continuity of the security applications in own area of responsibility, by developing BCP plans and ensuring that they are tested annually.

#### Security Analyst / Consultant

Previously involved in the Information Security and Encryption environment, which included determining the encryption requirements on various projects and assisting in implementing these requirements, mainly in the OS/390 or MVS environment. In addition, was required to provide advice to technical personnel on all aspects of the encryption environment.

#### Duties included:

- Project management for technical projects within the encryption environment.
- Analysis, design and programming of encryption requirements on the mainframe platform.
- Analysis and design of encryption requirements on the Internet and Stratus platform.
- System monitoring and tuning of current encryption areas.
- Key management co-ordination with various companies and internally.

#### **Information Audit Programmer**

Responsible for supporting the Security Analyst's by providing tools to enable them to audit the security environment. Also involved in implementing a decentralized security system for IT staff to utilize in obtaining and monitoring their access requirements.

#### Duties included:

- Analysis, design, programming and support of an 'above the line' decentralized security system.
- Implementation, training and maintenance of the above security system.
- Training of a new programmer to take over support of the Information Audit function.
- Design, programming and support of security programs required by the analyst's in order to audit the environment.