AST/ec/22.1.02
MS/SUP/DINERS/DI2518-R36-M J DAVIDSON2

# 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 MICHAEL JOHN DAVIDSON

**BE PLEASED TO TAKE NOTICE** that **MICHAEL JOHN DAVIDSON** will, at the hearing of the trial of this matter, give expert evidence on behalf of the Plaintiff as hereinafter set forth.

1. The expert witness understands The Standard Bank of SA Ltd's ("SBSA") ATM processing and Auto Bank card management system, and their interaction with other systems. He is responsible for developing mainframe application software and ensuring that it meets SBSA's requirements in terms of functionality, performance and integrity. Where these applications are required to interact with

different hardware or software he has been responsible for ensuring that these interfaces operate correctly.

2. The witness is presently a Computer Software Consultant in the employ of SBSA in the ATM development area.

3. The witness has been advised that:

3.1. The Plaintiff implemented a system of Personal Identity Numbers ("PINs") for use with the cards issued by the Plaintiff to its cardholders;

3.2. Generation of PINs is implemented on the SBSA infrastructure, that is, on the mainframe computer utilised by SBSA for purposes of generating PINs *inter alia* for Diners Club;

3.3. Diners Club International Service Centre ("DCISC"), based in the United Kingdom, created three component parts which, when added together, made up the Zone Master Key ("ZMK");

3.4. Three components were sent by DCISC to the Plaintiff and, more particularly, to three representatives of Plaintiff;

3.5. The respective components of the ZMK were, in a secure manner, entered into the SBSA mainframe computer;

3.6. The tape which SBSA receives from the Plaintiff containing *inter alia* the account numbers of members whose applications have been approved is delivered by courier on behalf of the Plaintiff to SBSA.

4.

4.1. The operation of the mainframe computer is the same now as it was in 1993, save to the extent that new systems have been programmed to convert the encryption process to a new and more sophisticated system.

4.2. 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 delivered by the Plaintiff to SBSA as aforementioned. In order to do this the tape is loaded onto the SBSA computers and at a pre-designated time the encrypted PIN in relation to each new cardholder is then recorded on a similar tape and the two tapes are returned by SBSA to the Plaintiff.

4.3. The operations department of SBSA transposes the encrypted PINS onto the output tape (which, as aforesaid, is a different tape to the one received by it from Plaintiff) and returns the two tapes to the Plaintiff.

4.4. The Plaintiff, thereafter, returns SBSA's tape to it and it recycles the tape.

4.5. The principles of good Key Management are followed and maintained.

4.6. SBSA does not store any PIN information on its mainframe computers or elsewhere.

4.7. SBSA issue non-random PIN numbers. Such a PIN is referred to as a "*derived PIN*" as opposed to a "*random PIN*". When the mainframe computer is asked to verify a PIN it is obliged, because the PIN is not stored, to recreate the PIN it responds either positively or negatively. The PIN will always be the same by virtue of it being non-random.

5.

5.1. A zone is created between SASwitch and SBSA and the Issuer Working Keys ("IWK" or "IWK's") and Acquirer Working Keys ("AWK" or "AWK's") and are changed programatically after re-establishment of communication between the SBSA and SASwitch systems.

5.2. The zone keys between SASwitch and SBSA are changed every year.

5.3. SBSA has dedicated lines between SASwitch (X.25) and its mainframe computers. The use of a Diners Club card at an ATM travels directly on that line from SASwitch to the SBSA mainframe computer for verification, in the case of a local transaction.

5.4. The ATM, belonging to another financial institution, encrypts the PIN using the Terminal Pin Key ("TPK") which it communicates to the acquired branch. There the encrypted PIN block is translated from encryption under the TPK to encryption under the AWK which is then communicated to SASwitch where the PIN Block is again translated using the IWK and communicated to SBSA's mainframe.

5.5. After the PIN has been verified by the mainframe a request is sent to the Plaintiff to authorise the transaction. The PIN Block is not, however, transmitted for this purpose. If, for any reason, the line between SBSA and the Plaintiff is down, SBSA stands in for it and authorises or declines the transaction based on information communicated to it by Plaintiff as referred to in paragraph 5.7 below.

5.6. The Plaintiff responds to the request either negatively or positively which response is then communicated through SBSA's mainframe, SASwitch, and the acquirer bank's mainframe to the ATM.

5.7. The tape which is sent to SBSA by the Plaintiff, referred to above, contains what is referred to as *"negative files"* as well as the account numbers for which the PINS are to be generated. The purpose of the negative files is to facilitate SBSA standing in when the Plaintiff is off line.

6.

6.1. The request by a card member for the issue of a PIN is received from the SBSA branch and is made directly to the mainframe computer.

6.2. The mainframe responds to the request and transmits the PIN, which it recreates against the PAN, and sends it to the SBSA branch making the request.

6.3. All issues of PINS are logged and a record thereof kept.

6.4. In the case of card number 36135828226037 there was only a single issue of the PIN on the 16th February 2000.

7. The PIN verification on the SBSA mainframe is performed utilising the IBM 4753, "black box" which is a tamper resistant Cryptographic engine.

8. On the basis of the aforegoing, the witness will express the following opinions:

8.1. At the time of the generation of the PINS i.e. on receipt of the tape from the Plaintiff, such generation in its encrypted form is, for all practical purposes, inviolate.

8.2. The PIN in the process of translation, communication and verification is inviolate in that the PIN is never released in the clear. ? ?

8.3. In his view no third party could have penetrated the SBSA system and obtained the clear PIN in respect of the First Defendant. In his experience the SBSA system has never been attacked and the encryption process prevents third parties from gaining access.