**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 DONALD JARDINE**

BE PLEASED TO TAKE NOTICE that **DONALD JARDINE** 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 "DJ1".

2.   The witness is presently the programmer for the Microswap/Auto E division of The Standard Bank of South Africa Limited ("SBSA").

3.   One of the facilities Auto E Centres offer is that it is able to issue Personal Identification Numbers ("PIN" or "PINs") and for that purpose communicates with the SBSA mainframe.

4.   A Diners Club member seeking to acquire his PIN approaches the SBSA branch in question together with his card and identity book. He is required to fill in a form and his signature is checked against both the card and his identity book or other acceptable identification.

5.   The form is presented to an operator in order to request the Auto E machines to retrieve the PIN. There is a particular designated level of "sign-on" for the persons requesting the PIN information. These levels of "sign-on's" depend on the level of security performed by the particular function. The level of "sign-on" is given to employees depending on the authority accorded them by SBSA.

6.   The supervisor has a Supervisor Sign-on, which is used to "sign on" and is of a higher security level than, for example , the operator.

7.   The steps taken to retrieve the PIN in an Auto E are as follows:

   7.1   The operator "signs on" with a secret code;

   7.2   An E14 request is then sent to the SBSA mainframe;

   7.3   The operator is then requested to enter a user ID and password;

   7.4   The Plaintiff's member's card is swiped in order to convey his Primary Account Number ("PAN") to the mainframe;

   7.5   The supervisor is then required to provide an override by supervisory sign-on swiping his card which constitutes authorisation for the action;

   7.6   The mainframe verifies the request and thereafter transmits the PIN which is then printed out in a secret PIN mailer by a dotmatrix printer.

8. More particularly:

    8.1 The PIN is communicated from the mainframe to a server, which uses a Convergent Technology Operations System ("CTOS"), located at the Auto E Centre.

    8.2 The line on which the communication takes place is a leased and dedicated line.

    8.3 The server communicates the PIN to a Print SPOOLER background function which is scheduled on the server in order that the PIN can be sent to the printer.

    8.4 Once the SPOOLER has communicated with the printer and the printer has completed printing, SPOOLER erases the data.

    8.5 The whole process from the time that the data in the CTOS server is sent to the printer and the printer completes the printing of the PIN and the data is deleted from the SPOOLER function takes, in the ordinary course, a matter of seconds.

9. The witness will express the following opinions based on the aforementioned and for the reasons appearing hereunder:

    9.1 In his opinion the system is secure and he knows of no instances where it has been breached. The system is complex and would require a very high level of skill, competence and sophisticated equipment to interfere therewith. Furthermore any attempt to physically interfere with the CTOS server, SPOOLER, or printer would be obvious to anybody in the branch.

    9.2 In his view it is inconceivable that a third party would attempt to unlawfully access either the PAN or PIN at the Auto E centre, not only for the reasons mentioned above but also because the

Bank has built into its operating system various safeguards to ensure that there is no tampering therewith.

9.3   In his view the line between the mainframe and the CTOS server is inviolate and to his knowledge has never been subjected to attack. There are 140 Auto E's in the Republic of South Africa and all have their own leased line. This would mean that access would have to occur either at the Auto E or at the mainframe and, as stated previously, this, in his view, simply could not happen. Furthermore the information is communicated via an NTU set which is not "dial-in" based. It has a permanent link with fixed terminal points. The server is always plugged in to the NTU and would have to be unplugged before a "hacker" could plug in. The server is sited right in front of the customer, the operator and the supervisor and anybody attempting to interfere therewith would have to physically plug and unplug the line which would be clearly visible. If anybody had been able to "hack into" the information being transferred from the mainframe computer, which, as previously stated has not, in his view, been violated, by virtue of the difficulties and costs involved, it is highly unlikely that the attack would have been restricted to one card and its associated PIN.

"DJ1"

CURRICULUM   VITAE

DONALD   JARDINE

December 1976	:	Matriculated Selborne College East London
December 1976	:	Joined Standard Bank of South Africa, East London Branch
July 1977 to June 1979	:	National Service
June 1979 to January 1983	:	Branch Teller / Computer Systems Liaison Officer
1983	:	Rhodes University
January 1984 to January 1986	:	Standard Bank Implementation Officer. Implemented branch accounting system on CTOS hardware in the rural areas of Standard Bank's branch network
February 1986 to May 1986	:	Van Zyl & Pritchard Cobol Programming Course
May 1986 to January 1990	:	Programmer on the Standard Bank's Micro Branch Accounting System which used the CTOS hardware platform. Designed, programmed and implemented various systems and projects
January 1990 to January 1995	:	Helped design, program and implemented the Standard Bank's Microswap Branch System. This eventually became the basis of the Auto E System
February 1995 to January 1997	:	Joined the African Banking Group of the Standard Bank. Designed, programmed and implemented various branch delivery systems for their banks in a variety of different African countries
February 1997 to date	:	Rejoined the Microswap / Auto E section as Senior Technical Consultant. Designed, programmed and implemented various projects and systems. Also maintained the current installed base. The systems maintained included the operating software, application software, host communications as well as hardware trouble shooting