AST/ec/12.12.01
MS/SUP/DINERS/DI2518-R36-PINNOCK

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 MICHAEL PINNOCK

TAKE NOTICE that

MICHAEL PINNOCK

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 a copy of the curriculum vitae of **MICHAEL PINNOCK** is annexed hereto marked "MP.1".

TAKE NOTICE FURTHER that the testimony of **MICHAEL PINNOCK** will be as hereinafter set forth.

BACKGROUND FACTS

1 The Standard Bank of South Africa Limited ("SBSA"), during 1992, established the necessary computer infrastructure to accommodate the installation of the component parts which, once combined, would result in the creation of a Zone Master Key ("ZMK").

2 The necessary component parts were generated by Diners Club International ("DCI") and transmitted to the plaintiff separately, the expert believes, in 1993.

3 Three different representatives of the plaintiff were furnished with a separate component in order to ensure the security of the process required for purposes of establishing the ZMK.

4 Each such employee of the plaintiff was called upon, in isolation and without reference to the other two employees, to *"input"* the component allocated to him into SBSA's mainframe computer.

5 Once each of the three employees had performed the task required of them, the SBSA mainframe, as aforesaid, combined the three elements and, in so doing, created the ZMK.

6 The expert was present at the time that the ZMK was established in this manner.

7 The reason that it was necessary for the ZMK to be established in the SBSA mainframe computer was that the ZMK so established had to correlate identically with the ZMK used by DCI in its computer systems. Bearing in mind that the tape of data generated by SBSA (which includes the encrypted PIN block) on behalf of the plaintiff is sent, the expert has been advised, by courier to DCI in the United Kingdom, it is only on the basis that DCI has loaded onto its computer systems the identical ZMK that DCI's systems are able to read the tape supplied by the plaintiff.

8 The decryption of the information stored on the tape received by DCI from the plaintiff takes place in consequence of the application by DCI's systems of the identical ZMK to the data stored on the tape and could only take place if the ZMK was identical to that employed by SBSA at the time that the tape was initially generated.

9 In order to ensure the security and integrity of the ZMK both at the SBSA mainframe computer and at the computers employed by DCI, the keys are stored in hardware based tamper proof cryptographic *"black boxes"*.

10 Once the ZMK has been established on the computer (irrespective of whether that be SBSA's computer or DCI's computer), the component parts used for purposes of establishing the ZMK are destroyed in order to ensure the continued and continuing integrity of the ZMK.

11 The creation of the ZMK by the introduction of the three component parts aforesaid into the computer system in question takes place in accordance with industry standards and practice, as does the destruction of the component parts.

THE EXPERT'S OPINION AND REASONS THEREFORE

12

12.1 **The expert's opinion**

The establishment and maintenance of the ZMK is not susceptible to either malfunction or third party interference or manipulation and secures the integrity of the PIN generation, the transmission of the encrypted PIN and the translation of the encrypted PIN by DCI for purposes of storage on the computer systems employed by DCI.

12.2 **The expert's reasons for the opinion**

The methodology employed in the creation of the ZMK and the standards to which the respective parties adhere are such as to ensure the integrity and security of the ZMK and are such as to render it insusceptible to either third party intervention or unauthorized access.

"MP1"

CURRICULUM VITAE

MICHAEL JOHN PINNOCK

IDENTITY NO. 321030 5016 08 3

PERIOD	POSITION HELD	COMPANY
Post Matric	Worked on gold mine, qualified as a Metallurgical Chemist. Hold a Govt. Certificate of Competency-Assaying	
National Service	Pilot - Rand held : Lieutenant Flying Instructor	South African Air Force
1960 - 1964	Secretary	Associated Scientific & Technical Societies of South Africa
1965 - 1968	Computer Salesman	Burroughs Machines Ltd
1968 - 1972	Data Processing Manager	Gillette Company, South Africa
1972 - 1973	Data Processing Manager	Color Processing Laboratories
1973 - 1975	Market Research Affiliate & Assistant Data Processing Manager	Lilly Laboratories SA Ltd
1975	Business Analyst/Consultant	Marshall Brooke, Simon & Associates
1975 - 1978	Data Processing Manager	Peugeot & Citroen SA
1979 - 1981	Group Data Processing Manager	Quinton Hazell-Superite Holdings
1981 - 1982	Systems & Facilities Consultant	Polygon Systems
1982 - 1983	Information Services Manager	Mega Plastics (Pty) Ltd
1983 - 1985	Product Manager (MVS Software)	George Kendall (Pty) Ltd
1983 - 1987	Security Consultant to Standard Bank for main frame security	George Kendall & 1987 M.D. Griffin Security Systems (own Coy)
1988 - 1996	Manager, Computer Security Dept	Standard Bank of South Africa
1996 - 1998	Information Security Consultant - Information Encryption Support - Information Security Architect	Standard Bank of South Africa
1998 - 2001	Information Security Consultant - Network & Encryption Services	Standard Bank of SA

Extra Mural : 1992 - 1998 : Studied Theology and in 1998 ordained Deacon, Roman Catholic Church

October 2001 : Qualified as Certified Information Systems Security Professional (CISSP)