AST/ec/16.11.01
MS/SUP/DINERS/DI2518-RULE36(9)(B)WALKER

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 ADRIAN WALKER

TAKE NOTICE that

ADRIAN WALKER

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 **ADRIAN WALKER** is annexed hereto marked "AW.1".

TAKE NOTICE FURTHER that the testimony of **ADRIAN WALKER** will be as hereinafter set forth.

BACKGROUND FACTS

1 All Automatic Teller Machine ("ATM") transactions arising in consequence of the use of a card issued by the plaintiff acquired in the UK are switched from Transaction Network Services (UK) Limited ("TNS") to a system called Card Authorisation Front End System ("CAFES"), which operates as a switch to RELAY for purposes of such transactions.

2 No verification or validation of the associated Personal Identification Number ("PIN") takes place at CAFES.

3 The expert has, since January 2001, been the manager of the technical support team for CAFES based in Farnborough in the United Kingdom.

INFORMATION OBTAINED

4 The expert has been advised that :

4.1 the plaintiff has instituted action against Mr Anil Singh, the first defendant, and Mrs Vanitha Singh, the second defendant, out of the High Court of the Republic of South Africa for recovery of monies disbursed by the plaintiff on behalf of the defendants; and

4.2 the action arises in consequence of the use of a Diners Club card and the associated PIN at various ATMs in and around London on 4 and 5 March 2000; and

4.3 a total of 199 transactions took place in consequence of the use of Diners Club card number 36135828226037 ("the card number") which was issued to the first defendant; and

4.4 of the 199 transactions aforesaid, 190 were successful, in that the ATMs in question dispensed cash on each such occasion. This would mean that 9 transactions failed, for whatever reason; and

4.5 the defendants contend, in defence of the action instituted against them, that neither of them utilized their Diners Club cards or facilities to receive any cash advances, to withdraw any monies from ATMs or to obtain travellers cheques on the dates alleged by the plaintiff, that is, 4 and 5 March 2000; and

4.6 the defendants further allege that neither of them was in the United Kingdom on the days in question, that is, 4 and 5 March 2000, that neither of them withdrew any of the sums alleged and that they accordingly deny liability to the plaintiff in respect of the alleged withdrawals.

THE OPERATION OF CAFES

5 TNS is *"upstream"* of CAFES, meaning that the information received by CAFES is sourced from TNS.

6 The information is transmitted electronically, it is encrypted (at least in part) and it is processed, that is, formatted and/or supplemented for purposes of onward transmission to RELAY in respect of a transaction emanating from the use of a card and PIN not issued in the UK. Insofar as a transaction emanating from the use of a domestically issued card and PIN (that is, a card and PIN issued in the UK) is concerned, the transaction is authorized by CAFES and does not get transmitted to RELAY. All transaction information generated through use of a card in the UK, irrespective of whether it arises in consequence of the use of a domestic or foreign card, however, is batched for billing and settlement purposes and sent to a system called Card Holder And Merchant Processing System ("CHAMPS").

7 CAFES is a Point of Sale/ATM acquirer and credit card authorisation system. CAFES runs on a Stratus computer hardware running the proprietary VOS operating system. The CAFES software application system is used by seven Diners Club franchises, including the UK franchise, to process authorisation transactions.

8 A retrieval reference number is allocated by CAFES to every transaction passed by it to RELAY.

9 CAFES, in addition, upon receipt of the information constituting a transaction, allocates to the information flow a trace number which, together with the information aforesaid, is passed on to RELAY as part of the *"information package"* relating to the transaction in question. The trace number allocated by the acquirer institution, however, is not passed on by CAFES to RELAY as part of the *"information package"*. The trace number allocated by CAFES when passing the *"information package"* onto RELAY is created by the Club Cash Interface between CAFES and RELAY and is an incremental number having the number 1 as its first digit and having five further digits ranging from the number 00001 to 99999.

10 In certain circumstances CAFES may not send on a transaction to RELAY. These circumstances can arise when a communication network failure occurs between TNS and CAFES, or a communication network

failure occurs between CAFES and RELAY, or a format error occurs on an authorisation request from TNS.

11 To the extent that CAFES constitutes an element in *"the route"* having, as its preceding element TNS and its succeeding element, RELAY, for authorizations and CHAMPS, for billing and settlement, the relationship between CAFES and its predecessor and successors is a function of electronic data received by it, processed by it and ultimately transmitted onward by it. The input data received by CAFES from TNS consists of the following :

11.1 the encrypted PIN block; and

11.2 the transaction information.

12 CAFES uses a Racal RG 7000 series hardware security module for purposes of decryption and re-encryption (that is, translation) of the PIN block. The Racal is connected to the host computer via an asynchronous communications link. CAFES and RELAY are in the same physical location.

13 The session keys used by CAFES, that is, the Link Zone Pin Key ("LZPK") and the Relay Zone Pin Key ("RZPK"), are stored under the Local Master Keys ("LMKs") for security purposes.

14 The billing or settlement information sent by CAFES to CHAMPS for onward transmission to INTERCHANGE is stripped of any data which does not specifically relate to the billing process, for example, the encrypted PIN block.

15 CAFES constructs a transaction for *"downstream"* RELAY based on the incoming information from TNS *"upstream"* and the only processing that takes place is the translation of the PIN block using the LZPK and RZPK assigned to TNS and RELAY respectively and the allocation of a Club Cash trace number.

16 A further point which it is necessary to appreciate is that CAFES operates, to an extent, as a filter and/or switch in that it recognizes Diners Club cards issued by Diners Club United Kingdom as being *"its own"* and identifies Diners Club cards which are not issued by Diners Club United Kingdom as being *"foreign"*.

17 Insofar as *"its own"* cards are concerned, CAFES is able to authorize the transaction in question without having to on-send the information any further. Insofar as a *"foreign"* Diners Club card is concerned, the authorization for the transaction is effected by RELAY.

18 CAFES and RELAY are both logically and physically split, that is, they run on different hardware platforms.

THE EXPERT'S OPINIONS AND REASONS THEREFOR

19

19.1 **The first opinion**

On the basis that the transactions in question were received by CAFES from TNS, the expert is of the opinion that the 194 ATM transactions to which he has previously referred took place in consequence of the presentation of a card whose magnetic stripe carries the authentic information which includes the card number and the derived PIN being present at the ATM simultaneously.

19.2 **The expert's reasons for the first opinion**

The CAFES Application systems in place have internal controls to ensure that illicit information injection cannot occur. It is not possible for any mechanism to masquerade as an ATM transaction originator. Within the expert's experience and to his knowledge a spurious or counterfeit transaction has never been injected into the

system and nor, for that matter, would the system be in a position, of its own accord, to generate such a transaction.

20

20.1 **The second opinion**

The integrity of the transaction data and the encrypted PIN block are inviolate both when they enter the CAFES application system and when they are processed and passed on to *"downstream"* functions, that is, RELAY.

20.2 **The expert's reasons for the second opinion**

The key management principles in place between CAFES and *"upstream"* TNS, as well as those with *"downstream"* RELAY adhere to the principles in the related ISO standards for such service. Tracking data is present in the data stream which is verified and/or added to at each one of the processing legs through which the transaction is routed. It enables manual verification of the occurrence of the transaction, should a query occur. The same tracking information is used in *"real time"*, that is, whilst the transaction is in progress, to ensure that the requests sent *"downstream"* are matched to the replies emanating from *"downstream"* in response to transaction requests.

21

21.1 **The third opinion**

The electronic data file automatically created by the CAFES application system for purposes of forwarding to CHAMPS contains billing and settlement records, each of which is a direct result of an ATM transaction and is a true and accurate reflection of the ATM transaction in question.

21.2 **The expert's reasons for the third opinion**

The recordal of the information on the batch file for onward transmission to CHAMPS is, in effect, contemporaneous with the transaction in question. This means that there would be no possibility of a spurious transaction or purported transaction being injected into the batch. This also means that a particular transaction can never be allocated as against the incorrect account. The record of transactions is a reflection of real time occurrences.

22

22.1 **The fourth opinion**

The LZPK and RZPK stored by CAFES are secure and are not susceptible to attack during their lifespan.

22.2 **The expert's reasons for the fourth opinion**

The LZPK and RZPK are stored on a data base encrypted under a pair of hardware security module LMKs. Even when the keys are in use, they are nonetheless immune from attack on the basis that they are imported into a so-called *"black box"* or Hardware Security Module, which is tamper resistant and in which they are decrypted for the period that they are required to translate the PIN block.

"AW. 1"

CV- Adrian Walker

Name : Adrian Walker
Date of Birth : 14th August 1960
Nationality : British
Education : 1978-1981
BSc (Honours) in Aeronautical Engineering
Bristol University, England

COMPUTER SYSTEMS SUMMARY

Operating Systems : UNIX: HP-UX, DEC-UNIX, AIX,
OTHER: STRATUS VOS

SOFTWARE : ORACLE RDBMS

Languages : C, C++, Java, PL/SQL, PL/1

WORK EXPERIENCE

February 1997 - Present

Diners Club International Service Centre (DCISC), Hampshire, England
Development Manager, Vice President

DCISC is the Operations centre for the Diners Club International Franchise network. I work as a Development Manager reporting to the Operations Director of DCISC.

Responsibilities include:

- Management of 8-10 Development staff
- Project Management
- Technical Design
- Technical Architecture and Strategic Planning
- Production System Operations Support

April 1993 - Febuary 1997

Citicorp Latin America Regional Technology Office, Florida USA
Technical Project Leader, Vice President.

The Latin American Consumer Bank Technology Office is responsible for the deployment of Citibank technology to Citibank Consumer in the Latin America region.

Responsibilities:

- Technical Project Management
- Technical Design
- Production Support and Technical Consultancy to Citibank Franchises in Latin American region

January 1990 - March 1993

Citibank Consumer Global Systems Division, New York City
Senior Systems Programmer, Assistant Vice President

The Global Systems Division was responsible for the development and support of ATM and POS Front-End Switch Systems for the International Citibank retail businesses.

Responsibilities included:

- Provision of technical consultancy and training for International divisions in Citibank.
- Systems Development on ATM Front End Switching Systems
- Systems Development for EFT/POS Interfaces in Credit Card Authorisation systems.

October 1988 - January 1990

FIRST BOSTON CORPORATION, New York City, NY USA
Consultant in the Information Systems Department

FBC were developing a multi-tiered case tool product, I worked as a developer working on the middle tier (Stratus VOS) part of the Case tool product.

January 1985 - October 1988

LOGICA UK London, England
Consultant

Worked on various projects both in-house and on clients sites.

January 1984 - January 1985

National Maritime Institute, Teddington, England
Research Engineer

November 1981 - January 1984

Marconi Underwater Systems Ltd
Research Engineer