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

SINGH, VANITHA

First Defendant

Second Defendant

PLAINTIFF'S NOTICE IN TERMS OF RULE 36(9)(a) AND (b) IN RESPECT OF THE TESTIMONY OF MICHAEL BIRD

TAKE NOTICE that

MICHAEL BIRD

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 BIRD is annexed hereto marked "MB.1".

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

BACKGROUND FACTS

- The expert is the development manager for certain applications software known as RELAY and INTERCHANGE based in Farnborough in the United Kingdom.
- The transactions that take place in consequence, for example, of a card issued by the plaintiff and its associated Personal Identification Number ("PIN") being used at an Automatic Teller Machine ("ATM") in the UK are routed through various computer applications software managed by the Diners Club International Service Centre ("DCISC") which applications:
 - verify the authenticity of the information received by it and the correctness of the associated PIN and, more particularly, by an electronic transaction, authorization and routing system known as RELAY; and

2.2 receive billing information from franchise card management systems, one of which is the Card Holder And Merchant Processing System ("CHAMPS") which routes the billing information to the system known as INTERCHANGE.

3 The expert has been advised that:

- 3.1 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
- 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
- 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
- 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 expert has been advised that 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.
- The expert has further been advised that of the 199 transactions aforesaid, 190 were successful (the expert, insofar as the successful transactions are concerned, having scrutinized the logs himself), in that the ATMs in question dispensed cash on each such occasion. This would mean that 9 transactions failed, for whatever reason.

6

1.

- The transaction log generated by RELAY, however, reflects only 194 transactions on the basis that certain of the transactions recorded elsewhere in "the route" were not ultimately received by RELAY, that is, five of the failed transactions.
- 6.2 INTERCHANGE, in its turn, receives a transaction file from, for example, CHAMPS, which information is then batched and sent on to the respective franchisees whose cardholders have used their cards anywhere in the world.

- 7 The 9 failures were, whether on the basis of information given to him or information derived from the transaction log aforesaid, declined on the basis that they:
 - 7.1 required an amount which was in excess of that which the parameters input into the application at the behest of the plaintiff could allow; or
 - 7.2 were not associated with the correct PIN being entered into the ATM in question; or
 - 7.3 were not recognized as valid transactions and therefore not passed to RELAY, for example, in consequence of an invalid account or service type having been selected.

THE OPERATION OF RELAY

The plaintiff sends a tape to the RELAY system which contains valid account numbers and Zone Pin Key ("ZPK") encrypted PINs, RELAY electronically reads in the file, extracts and stores the account numbers, extracts the associated PINs, and passes them to the HSM for translation from the ZPK to a pair of Local Master Keys ("LMKs") for storage.

- The Card Authorization Front End System ("CAFES") is "upstream" of RELAY, meaning that the information received by RELAY is routed from CAFES.
- The information is received from CAFES by RELAY electronically and in an encrypted form with respect to the PIN in order that the verification and authorization process might take place.
- 11 RELAY is in possession of the encrypted PIN which it received (via the electronically-read file) from the plaintiff (as generated by The Standard Bank of South Africa Limited) and is accordingly in a position to reconcile the encrypted PIN block received by it from CAFES with that stored in its data base. To the extent that the PINs reconcile, the PIN will be verified and, upon verification, processing continues, that is, the amount requested by the card user can be authorized if within the parameters prescribed by the plaintiff. In the event, however, that the PINs do not reconcile, the transaction goes no further and is declined.
- Transactions are either approved or declined. In the present instance the expert, as aforesaid, has examined the logs and is satisfied that there were no reversals.
- RELAY provides a transaction authorisation and switching service to card acquirers from POS, ATM and airline reservation services. Diners Club

card issuers can record details of their respective card bases in RELAY, which can then provide a validation service, including PIN checking in the event the card issuer has registered their PINs on the RELAY system. INTERCHANGE provides for the submission of charge billing data by acquirers to the card issuers by allowing validated input data to be made available for collection by the card issuer. INTERCHANGE also provides a mechanism for charging back disputed transactions.

- To the extent that RELAY constitutes an element in "the route", having, as its preceding element CAFES and its succeeding element the BRIDGE system at the plaintiff, the relationship between RELAY and its predecessor and successor is a function of electronic data received by it, processed by it and ultimately transmitted onward by it. The input data received by RELAY from CAFES consists of a message which contains transaction information and the encrypted PIN block necessary for authorization purposes.
- 15 RELAY uses a Racal RG 7000 series which communicates via an asynchronous protocol to its host computer.
- The Acquirer Working Key ("AWK") and Issuer Working Key ("IWK"), that is, the session keys are created by RELAY in accordance with accepted industry standard practice.

- The session keys aforesaid are stored, for their lifespan, in encrypted form, under the relevant Local Master Key pair ("LMK") of the Hardware Security Module ("HSM").
- No duplication of transactions takes place in RELAY, in that every transaction is seen as a unique event.
- 19 Upon receipt by RELAY of information relating to a transaction event, the system checks that :
 - 19.1 the card number in issue exists on its database; and
 - 19.2 the card number in issue has not been negatively marked, that is, that it does not constitute a card in respect of which no transaction will be allowed.
 - 19.3 the PIN associated with the transaction against the stored encrypted PIN and card number received from the plaintiff; and
 - 19.4 the expiry date of the card; and
 - 19.5 that the amount of the request is within the prescribed limits imposed by the plaintiff.

A further point which it is necessary to appreciate is that RELAY functions as a "stand in authorizer" with respect to "foreign" transactions for and on behalf of most franchisees and, in the present instance, on behalf of the plaintiff.

THE OPERATION OF INTERCHANGE

- INTERCHANGE receives data from CHAMPS, amongst other cardholder transaction data systems, in batched format relating to all those transactions which have taken place either at an ATM or at a point of sale ("POS"). If the transaction in question took place in a country other than the country out of which the card in question was issued, INTERCHANGE validates the transaction and/or a batch of transactions and makes the batch available for collection by the various franchisees, one of which is the plaintiff.
- For purposes of the present case, the transactions in question are those pertaining to the usage of a card bearing the card number issued by or on behalf of the plaintiff.
- The information batched by INTERCHANGE is electronically retrieved by the individual franchisees each day for subsequent allocation by the franchisees to the respective account holders.

- The batched information retrieved by the franchisee is used by the franchisees to formulate their statements in respect of its account holders.
- 25 INTERCHANGE and RELAY are both logically and physically split, that is, they run on different hardware platforms.

THE EXPERT'S OPINIONS AND REASONS THEREFOR

26

26.1 The first opinion

On the basis that the transactions in question were received by RELAY from CAFES and by INTERCHANGE from CHAMPS, the expert is of the opinion that the 194 ATM transactions (recorded by RELAY) and the 190 successful ATM transactions (as recorded by INTERCHANGE) to which he has previously referred took place in consequence of the presentation of a card whose magnetic stripe carried the authentic information which includes the card number and the derived PIN being present at the ATM simultaneously.

26.2 The expert's reasons for the first opinion

The 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.

27

27.1 The second opinion

The integrity of the transaction data and the encrypted PIN block is inviolate when they enter RELAY and when they are processed.

27.2 The expert's reasons for the second opinion

The key management principles in place between RELAY and "upstream" CAFES adhere to the principles and 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.

28

28.1 The third opinion

The customer PIN verification methodology is inviolate.

28.2 The expert's reasons for the third opinion

RELAY is designed to route PIN checking to the hardware device, that is, the hardware security module ("HSM"). If the HSM is inoperative or unavailable for whatever reason, the applications are designed to reject the transaction on the basis that PIN checking is not possible.

29

ħ

29.1 The fourth opinion

RELAY cannot randomly create its own data and is always dependent upon data which is received by it from an external source, in this instance, CAFES, for purposes of verifying and authorizing a particular transaction.

29.2 The expert's reasons for the fourth opinion

The functionality provided in the system is such that it can only react to incoming data, that is, it cannot create or recreate the incoming data string.

30

30.1 The fifth opinion

The AWK stored by RELAY is secure and is not susceptible to attack during its lifespan.

30.2 The expert's reasons for the fifth opinion

The AWK is 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 HSM, which is tamper resistant and in which they are decrypted for the period that they are required to translate the PIN block.

31

31.1 The sixth opinion

The PIN stored by RELAY is inviolate.

31.2 The expert's reasons for the sixth opinion

The PIN is stored under a double length Data Encryption Standard key.

M.B. 1

MICHAEL ANTHONY BIRD M.A., F.C.I.I.

EMPLOYMENT

Jan 1991- DINERS CLUB INTERNATIONAL

Provider of global financial message switching and authorisation service on behalf of the Diners Club community. A wholly owned subsidiary of Citicorp and a significant player in the plastic card industry.

Diners Club International Service Centre - Development Manager. This position is responsible for provision of DCI Global Operations support worldwide.

Responsible for a team of highly skilled people who provide the Operational support and Development of the International Authorisation and Charge Detail Interchange systems which connects 55 territories to the central computer system. I ensure provision of a non stop 24 hour automated authorisation service that customers obtain authorisations in a timely and efficient manner and that such charges are delivered for billing and interterritorial financial settlement. This job involves liaison with the various companies which comprise the Diners Club World, development of the system in support of Business needs, setting the strategic direction, providing Operational Support and advice as well as maintaining a Production service within the tight schedule demanded of International transaction flow. In addition I am responsible for the selection of appropriate hardware and software for and for liaising with outside suppliers of services, including the agreement of Service Level Agreements.

1983-1991 **TSB GROUP**

This important UK clearing bank group is a significant provider of an extensive range of banking and other financial services through its subsidiaries and a countrywide network of 1600 branches and 25,000 staff.

Jan 1990 - Jan 1991 TSB GROUP HEAD OFFICE, LONDON - Card Systems Executive

Responsible for monitoring developments in card processing systems and related technologies, identify, analyse and report to general management on trends and developments that will influence the card strategy of the retail banking arm of the Group.

Sept 1988 - Dec 1989 TSB TRUSTCARD, BRIGHTON - Head of Department P.O.S. Systems

Responsible for a team for technical development at TSB. Group Level and for delivery of the tested and working interface to the EFTPOS UK clearing system, planning and co-ordinating TSB's banking and card processing systems to provide a unified approach and resolving any unacceptable situations revealed. In addition project manage the implementation of the TSB's interface to the Eurocard/Mastercard networks and the issue of a brand new product to utilise the facility.

May 1987 - Aug 1988 TSB GROUP HEAD OFFICE, LONDON - EFTPOS Technical Support Executive

Responsible for the integration of the Group's operating companies' entry into the EFTPOS UK Project, creation of specification documents, agreement on appropriate standards, co-ordination of the technical aspects and TSB contact with external organisations. Acted as interface between the Group operating companies and EFTPOS UK ensuring that all technical activities, plans and effort were directed to a common goal.

Jan 1984 - May 1987 TSB TRUSTCARD, BRIGHTON - Business Support Manager

Originally a part of a team setting up the Group's credit card processing service, the position was effectively project management involving liaison and negotiation with user departments, suppliers and the establishment of budgets. Significant projects were the establishment of a plastic card production centre and PIN issuing facility and the implementation of ATM reciprocity systems within the bank and externally to the VISA ATM network.

i-As Business Support Manager my principal responsibility was to analyse user project proposals which necessitated directing studies to assess the viability and business/technical implications of new business support systems, one of which was EFTPOS which led to my next promotion.

Reporting to the Chief Inspector I was responsible for the creation of a new function in the bank (as systems had not previously been subject to internal scrutiny), establishing procedures and systems. Coincidentally the preparation of the 18 TSB's in England and Wales for floatation led to the centralisation of the Retail Bank's computer activities and the closure of the TSB South East computer centre thus enabling me to move to Trustcard and fulfil my ambition to move from Audit into Systems Development.

Aug 1972 - June 1983

COMMERCIAL UNION ASSURANCE GROUP - One of the larger composite insurance companies in the UK.

Jan 1981 - June 1983 Senior Internal Auditor EDP - London.

I was responsible for leading teams to investigate, review and report upon the company's computer systems worldwide.

I was seconded for nine months to organise all administrative aspects of the Sixth World Congress on Insurance Law in London, covering the venue and entertaining an accommodating 1200 delegates from all parts of the world. Planning, co-ordinating and many other areas of learning at this event enhanced my experience.