

74  
45.  
IN THE HIGH COURT OF SOUTH AFRICA

DURBAN AND COAST LOCAL DIVISION

CASE NO: 3156/2000

IN the matter between:-

DINERS CLUB

Plaintiff

and

ANIL SINGH

First Defendant

VANITHRA SINGH

Second Defendant

---

DEFENDANTS' AFFIDAVIT

---

I, the undersigned, ANIL SINGH do hereby make oath and state that:-

1.

I am the First Defendant herein and depose to this Affidavit on my own behalf and on behalf of the Second Defendant.

2.

I have read the application in this matter.

3.

Both the Second Defendant and I oppose the relief claimed herein. We have accordingly been advised that it is necessary for an Affidavit to be delivered in which the bases of our opposition is set forth. I accordingly depose to this Affidavit.

4.

In the interests of brevity and also due to time constraints, I have been advised that it would be acceptable if I do not traverse each and every allegation made in the Affidavit of MR. BOND and in the supporting Affidavit of MR. KENNEDY. Suffice to say that my not doing so must not be construed as an admission by us of the correctness of each and every allegation therein contained. Where such allegations are in conflict with the contents of this Affidavit (or the tenor hereof) or in conflict with the allegations to be made in an Affidavit to be deposed to by DR. ROSS JOHN ANDERSON of Cambridge, United Kingdom, we deny the same.

5.

I take issue with the suggestion contained in the application to the effect that the Second Defendant and I are mala fide. As I understand it, such a suggestion is based on the fact that a Rule 36 (6) Notice was served on 27 August 2002 and no

AS

response has been received to the demand contained in the Plaintiff's Attorney's letter dated 6 September 2002 (Annexure "CB 1").

6.

I respond as follows:

6.1. The allegation that we "threatened" to serve such a notice at the postponement of the matter on 24 June 2002 is, on what I have been advised by my Legal Representatives, incorrect. When the matter was last heard by this Honourable Court, I am advised that in the Chambers of His Lordship presiding, my Senior Counsel mentioned in passing, in the presence of the Plaintiff's Counsel, that:-

6.1.1. an extremely hurried trip had been made by us to the United Kingdom, to consult DR. ANDERSON and thereafter, expert notices were prepared and delivered under considerable time constraints;

6.1.2. an application for evidence to be heard on commission had also to be prepared (which was adjudicated upon by His Lordship presiding and an order thereon obtained, by consent);

(Both the foregoing aspects appeared from or could have been concluded, in any event, from the application for evidence on commission and the expert notices delivered on our behalf.)

6.1.3. additional discussions would be taking place between my Legal Representatives and DR. ANDERSON, whereafter a notice in terms of Rule 36 (6) for inspection of the computer systems relied upon by the Plaintiff, a request for particulars for trial and a notice for additional discovery would be served. This was not in the form of a threat but was mentioned in passing;

6.1.4. the Plaintiff's Senior Counsel responded that the Plaintiff would not accede to any request for inspection of computer systems and at that point in time His Lordship presiding intervened and brought the discussion to an end indicating quite clearly that he would deal with the merits of any such matters if and when they were placed before him;

6.1.5. nothing further, in relation to such notices was then mentioned. The foregoing, particularly because it

AD

occurred in the presence of His Lordship presiding,  
could hardly be construed as a threat.

6.2. Subsequent to the matter being adjourned, certain without prejudice discussions ensued between the respective Counsel, in consequence of which we were requested to consider whether we would be prepared to enter into negotiations for a settlement of the dispute. This required consultations, careful consideration and additional input from DR. ANDERSON, before we could make a decision. Our decision was that we were not prepared to settle the matter and that we wished this Honourable Court to decide the same.

6.3. By the time all the foregoing had occurred (DR. ANDERSON was also out of the United Kingdom until the first week of July 2002) some two to three weeks had elapsed. Thereafter, my Legal Representatives communicated with DR. ANDERSON on a few occasions and no doubt due to pressure of work on the part of my Legal Representatives and on the part of DR. ANDERSON, DR. ANDERSON was only able to properly apply his mind to what information ought to be requested, what additional documents ought to be discovered by the Plaintiff and what equipment ought to be requested for inspection during August 2002. In consequence, the notices and request for particulars referred to above, were only ready and served on 27 August 2002.

57.

6.4. I do not understand why it is suggested that because His Lordship would be on leave from the beginning of October 2002 until the end of the year (or perhaps the end of January 2003) the service of the foregoing on 27 August 2002 results in any mala fides on our part. It is quite clear, in my respectful submission, that approaches could have been made to His Lordship upon his return from leave, to entertain this matter at the beginning of February 2003. In any event, it was also possible (as indeed has happened) that arrangements could be made for His Lordship to hear this matter before His Lordship went on leave.

6.5 In any event, I was advised by my Legal Representatives (and if the advice I have received is incorrect, I sincerely apologise therefor) that having caused the Rule 36 (6) notice, the Rule 35 (3) notice and the request for particulars for trial to be served, we were, in respect of those notices and request, dominus litis, and a decision to take any of these matters any further would rest with us. Instead, the Plaintiff has sought to disregard this and has prepared an urgent application to be heard by this Honourable Court.

6.6. In addition, insofar as the request for particulars for trial is concerned, the Plaintiff is apparently adopting the attitude that it is not obliged to respond to the same due to the fact that Uniform Rule 21 provides for such a request to be served "before" trial and the request in the present

AD

case has been served "during" the trial.

6.7. I annex hereto marked "VS 1", a notice in terms of Rule 30, dated 11 September 2002, received by our Attorneys from the Plaintiff's Attorneys, the contents whereof I respectfully submit are self explanatory.

6.8. In the aforesaid notice my Legal Representatives have been informed that the Plaintiff intends, unless we withdraw such request for particulars for trial, to move an application in terms of Rule 30, to set such request for particulars aside as being an irregular step. The Plaintiff will no doubt prepare and move such an application immediately upon the expiry of the notice period in the aforesaid notice. As this matter has been brought before this Honourable Court, we now take this opportunity of humbly requesting this Honourable Court to grant an order in favour of the Second Defendant and I either authorising/condoning the delivery of the said request for particulars for trial, or alternatively, granting us permission to deliver such a request for particulars for trial, in which event we will cause the request already delivered to be withdrawn and an identical request to be served.

6.9. Our request is based on the fact that (as this Honourable Court is also aware, having acceded to a request by us for an adjournment of the

matter in March 2002) we were not in the position of being able to obtain the services/opinion of a suitable expert and consequently, neither the Second Defendant nor I (nor our Legal Representatives for that matter) were aware of the additional information/documents/access to equipment, which would be necessary to properly and adequately put forward our defence and refute the Plaintiff's contentions.

6.10. After the matter was adjourned, to enable us to obtain the services of such an expert, we have indeed done so. Acting on his advice, we now realise that we require additional information, which is encompassed in the request for particulars for trial (a copy of which will be before this Honourable Court in the Court file in this matter) and as the trial of the matter is still more than five months away from being recommenced, we submit that the Plaintiff will suffer no prejudice in responding to the same. On the other hand, if we are not allowed to request pertinent information, we will be severely prejudiced in this matter.

6.11. In requesting as aforesaid, we do not wish it to be thought by this Honourable Court that we suggest it should consider the request for particulars itself, on 26 September 2002 and direct the Plaintiff to respond to any or all of the questions therein. It has been agreed between the respective Senior Counsel that this Honourable Court will not be requested to decide upon the same, at this stage. Should we



receive permission to deliver such request and should the Plaintiff decline to furnish the information sought or not furnish the same adequately, an appropriate application can then be considered and launched (if necessary) to be heard by this Honourable Court in February 2003, when His Lordship returns from leave.

6.12. Insofar as not adhering to the demand contained in the letter of the Plaintiff's Attorneys dated 6 September 2002 is concerned, we respectfully submit the following:

6.12.1. Uniform Rule 36 (7) affords to the Plaintiff an opportunity of requesting us to specify the nature of the examinations to which it is proposed that the items be subjected.

6.12.2. Adequate opportunity must be afforded to the recipient of such a request to furnish the information sought.

6.12.3. Just after the said letter was received by our Attorneys, the Plaintiff's Senior Counsel communicated with our Senior Counsel with a view to ascertaining whether we would be agreeable to this matter being heard by this Honourable Court before the end of September 2002,

which consent was supplied forthwith. Accordingly, the Plaintiff had already, at that stage, made up its mind that it was bringing such an application, unless we withdrew the notice.

6.12.4. In any event, in the said letter the Plaintiff's Attorneys record that the state or condition of the items listed in the said notice are not relied upon by the Plaintiff. They furthermore record that such property was not in their Client's control and possession. Notwithstanding this, they proceed to "demand" that the nature of the examination be specified and record that if we did not adhere to that demand, this Honourable Court would be asked at the hearing of the application to draw an inference that we are mala fide. Furthermore, the service of the Rule 36 (6) notice cannot, in my respectful submission, be construed as being "in terrorem" as all the Plaintiff had to do was to decline to submit the items requested to the inspections, whereafter, in terms of Rule 36 (7), a Judge in Chambers would have had to decide the matter, if we elected to proceed further with this matter.

6.12.5. As His Lordship presiding is already familiar with various aspects of this case, we too would have preferred that an adjudication on the Rule 36 (6) notice be undertaken by him and had the Plaintiff allowed the matter to proceed in terms of the Uniform Rules, we would have suggested as much to it, if we decided to proceed further. In any event, the Plaintiff could always have requested that the matter be placed before His Lordship presiding when it refused the inspections sought.

6.13. Far be it from the Second Defendant and I being mala fide and acting in terrorem, the tenor of the letter itself in my respectful submission shows who is attempting to intimidate whom.

6.14. We do not accept the correctness of the Plaintiff's contentions, namely that the items we seek to have inspected must be in the Plaintiff's possession or under its control for us to request an examination of the same. We also do not accept that the Plaintiff does not (or will not) rely upon the said items in this case. This was demonstrated, in my respectful submission, by the Plaintiff's Counsel putting the content of the various expert notices of the Plaintiff's experts to our witness MR. GIBSON and asking him whether he took issue with any of the

same.

6.15. It is our further respectful submission that a reasonable opportunity must be afforded to a litigant to furnish details requested by the other side. The service of the letter on 6 September 2002 and the demand contained therein, the aforesaid communication by the Plaintiff's Senior Counsel with our Senior Counsel shortly thereafter (to obtain consent for the matter to be heard before the end of September 2002), the request to His Lordship for the matter to be enrolled on a suitable date before the end of September 2002 and the actual bringing of the application (the notice of motion is dated 14 September 2002 and it was served on 16 September 2002) resulted in the Second Defendant and I having, effectively, five working days to adhere to the demand, and furnish the information sought (and even if we had the Plaintiff would still have launched this application). It will also be noted that the letter, served on 6 September 2002, demanded that we comply on the next working day (9 September 2002). The Plaintiff was well aware that we rely upon the expertise of expert witnesses in the United Kingdom.

6.16. The result of this application being enrolled for hearing is that we and our expert DR. ANDERSON have been prejudiced with shortage of time within which to properly deal with each and every allegation made in the affidavits under reply.

6.17. Notwithstanding this, in view of the fact that His Lordship presiding has been inconvenienced and has had to obtain permission to hear this matter in Pietermaritzburg (I am advised that His Lordship is for the month of September attending to criminal matters in Pietermaritzburg and this is a Durban matter) we do not wish to cause any further inconvenience and for that reason will endeavour to persuade this Honourable Court to refuse the Plaintiff's application on 26 September 2002 and at the same time to grant us appropriate relief in respect of the request for particulars for trial referred to above.

7.

In all the circumstances I respectfully submit that there is no basis whatsoever for the Plaintiff to suggest that the Second Defendant and I are mala fide or that we are acting in terrorem.

8.

We have, through our Legal Representatives, requested DR. ANDERSON to respond (as best he can, given his considerable work schedule and the time constraints placed upon us) to the allegations in the application and to set forth in an affidavit, the nature of the examinations/inspections which it is proposed the items will be subjected to. We have also requested him to deal with other salient aspects pertinent to the Rule 36 (6) notice, the Rule 35 (3) notice and the request for particulars for trial. We humbly request this Honourable Court to accept a



facsimile copy of the said affidavit which was deposed to in the United Kingdom, given the urgency of this matter. The said affidavit was received by facsimile, at the Chambers of our Senior Counsel, after close of business on Friday 20 September 2002 and came to his attention on the morning of Monday 23 September 2002.

9.

Insofar as the merits of the application and the necessity for the inspection of the systems relied upon by the Plaintiff are concerned, I respectfully refer to the content of DR. ANDERSON's affidavit and in addition I state:

9.1. Even if the Plaintiff is correct in stating, as it does in paragraph 3 of the affidavit under reply, that the Plaintiff relies upon a certificate given under the hand of MR. PROSPERO and that it does not rely upon the state or condition of any systems, this cannot be correct in the context of this matter.

9.2. This Honourable Court will recall that even prior to the hearing of this matter, the Plaintiff sought and obtained an order for the hearing of the evidence of its expert witnesses in the United Kingdom, on commission.

9.3. On 24 June 2002, by consent of the parties, this Honourable Court agreed to His Lordship presiding acting as Commissioner and taking



the evidence of the Plaintiff's expert witnesses in the United Kingdom, after the evidence of DR. ANDERSON and his colleagues has been given. His Lordship will then, as I understand it, come back to South Africa and after hearing argument, rule on whether such evidence of the Plaintiff is admissible, given that the Defendants contend that the Plaintiff is not entitled to lead any evidence in rebuttal.

9.4. That being so, the Second Defendant and I will be seriously prejudiced if expert testimony (which is subject to cross examination) is delivered and recorded and later ruled admissible without our experts and Legal Representatives being afforded a full and proper opportunity of testing the claimed inviolability of the computer systems upon which the Plaintiff relies and putting to the Plaintiff's expert witnesses (all of whom will apparently testify as to the inviolability of systems) any shortcomings which might be found to be present. In addition, the testimony of the Defendants' experts will have considerably more impact and weight behind it if they are able to pin point shortcomings in any of the systems upon which the Plaintiff must, of necessity, rely. On the other hand, if the systems are indeed inviolate, that will, in short, be the end of the case. DR. ANDERSON will no doubt testify as to the shortcomings in the systems or the absence thereof. Rule 36 (8) directs that a report of the examinations/inspections must be delivered and thus the Plaintiff will be well aware, prior to the recommenced



hearing, of the outcome of the examinations/inspections. Our witnesses can also be cross-examined thereon. The costs of such examinations/inspections must also be borne by us, in terms of Rule 36 (8) and the Plaintiff can suffer no prejudice in that regard.

9.5. To deprive us of the right of having the systems subjected to proper examinations/inspections by persons who are clearly experts of the highest calibre, would be to deny us a fair trial and would also not be in the interests of justice.

9.6. I respectfully submit that the Plaintiff cannot be correct in suggesting that where it has used various organisations and their computer systems to process transactions which at the end of the day are debited to my account, the Court must accept the word of the Plaintiff's experts (almost all of whom are employed by the various organisations involved in the entire transaction network) without the very systems which they claim to be infallible being tested.

9.7. DR. ANDERSON deals, in further detail, with the relevance of the said examinations and the additional information and documents which are requested, in his affidavit, and this Honourable Court is humbly referred thereto. I am not an expert in the field of computing. Neither is the Second Defendant. We consequently cannot proffer any opinion on the



correctness or otherwise of the opinions of the Plaintiff's witnesses, that of DR. ANDERSON and his colleagues and the attempt by MR. C. BOND to discredit our experts. I respectfully submit that these are matters for adjudication by this Honourable Court and it is humbly requested to take into account that nowhere in the affidavits supporting this application do either of the deponents claim to be experts in the field of computing and therefore capable of criticising the expert testimony of DR. ANDERSON and his colleagues.

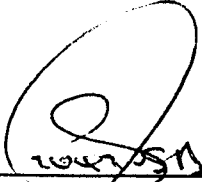
WHEREFORE the Second Defendant and I humbly pray that it may please this Honourable Court to dismiss the application to strike out the Rule 36 (6) notice with costs, such to include those consequent upon the employment of two Counsel, to grant us appropriate relief in respect of the request for particulars for trial delivered on 27 August 2002, or to grant such other relief as to it seems meet.

  
DEPONENT

I certify that the Deponent has acknowledged that he/she knows and understands the contents of this Affidavit which was SIGNED and SWORN TO at \_\_\_\_\_ BEFORE ME this \_\_\_\_\_ day of \_\_\_\_\_, 2002,



the Regulations contained in Government Notices Numbers R1258 of 21 July 1972 and R1648 of 16 August 1977, as amended, having been complied with.



COMMISSIONER OF OATHS 2002-98-23

FULL NAME: M. G. Mokoena  
SOUTH AFRICAN POLICE SERVICE

BUSINESS ADDRESS: Durban Central

CAPACITY: CS1

AREA: Durban



"V.S.I"

**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

**NOTICE IN TERMS OF RULE 30**

**BE PLEASED TO TAKE NOTICE** that Plaintiff intends applying to the above Honourable Court for an Order setting aside the Defendant's request for further particulars for the purposes of Trial dated 27<sup>th</sup> August 2002 on the basis that such request was not made in accordance with the provisions of Rule 21, the Trial having commenced on the 4<sup>th</sup> March 2002.

**FURTHER TAKE NOTICE** that unless Defendants remove the cause of complaint within ten days of the date of the delivery hereof application to set aside same will be made in accordance with Rule 30.

62

DATED AT *JH* ON THIS THE *11<sup>th</sup>* DAY OF SEPTEMBER 2002

(Sgd.) A.S.L. TURNER

**BOWES & TURNER INC**  
Plaintiff's Attorneys  
c/o **GOODRICKES**  
28<sup>th</sup> Floor, 320 West Street  
DURBAN  
Tel: (031) 301-6211  
Ref: Mr J A Allan

TO:

**THE REGISTRAR  
THE HIGH COURT  
DURBAN**

AND TO:

**J KISSOON SINGH INC**  
Defendant's Attorneys  
First Floor, International Plaza  
128/132 Commercial Road  
DURBAN  
Ref: Ms Patel/sb/03S944K01

Received a copy hereof this  
day of September 2002

For: Defendant's Attorneys

RECEIVED  
Date: *12-9-2* 10:17  
Signature: *RS*  
J. KISSOON SINGH INC

*MS*

CE

IN THE HIGH COURT OF SOUTH AFRICA  
DURBAN AND COAST LOCAL DIVISION

CASE NO. 3156/2000

In the matter between:

DINERS CLUB (SA) (PTY) LTD

Plaintiff

and

ANIL SINGH

First Defendant

VANITHRA SINGH


Second Defendant

---

AFFIDAVIT

---

I, ROSS JOHN ANDERSON, date of birth 15/9/1956, resident in Bedfordshire,  
England, do hereby make oath and state that:-

RC-

2

1. I have had very little time to prepare this affidavit (which I have done basically on my own, with only a little assistance from the defendant's legal representatives, in consequence of time constraints and distance) in response to the plaintiff's Notice of Motion for the hearing on the 26th September. I received the notice in the afternoon of the 18th September, and I have for some time been committed to appearing at a workshop at Schloss Dagstuhl, Germany, from 22-27 September. (This is public information, available on the web at <http://www.dagstuhl.de/02391/Titles/>.) The timing of the Notice has left me only the 19th and 20th of September to respond to it; other commitments constrain the available time still further.
  
2. Therefore, with respect, I am unable to reply to the affidavit of Craig Bond in detail. I have been advised to limit my reply to the reason why the defence needs further particulars, access to documents and access to equipment in order to ensure a fair trial; the nature of the examination of equipment and the tests to be performed; and just enough material in rebuttal of the plaintiff's claims to show that it has either failed to understand the defence expert notices, or is deliberately misunderstanding them in order to create confusion. I sincerely apologise for not being able to deal with this matter in as much detail as I would have preferred.

PC. 

66.  
67.

3. The essence of this case is that the plaintiff claims its systems and the systems of its associates are secure, and therefore the transactions made on the first defendant's account must have involved him using his card and the PIN issued to him, or allowing someone else to use them. The defendants deny having made the transactions or suffering them to be made. As the main defence expert, I have filed a notice explaining many of the ways in which ATM security systems, of the type relied on by the plaintiff, have failed in the past, and a number of specific vulnerabilities of the hardware security modules (HSMs) on which the plaintiff places particular reliance.
  
4. If the honourable Court needs a specific example of how the security systems failed in this case, one need only consider the fact that 199 transactions were made over a weekend, of which 194 succeeded. A secure ATM system would never permit this; only a few transactions would be allowed per day and per card. As I explained in my expert summary, this security failure appears to lie at the heart of the case. In order to understand what happened, the Court should know how this vulnerability arose, who knew of it, when they learned of it, and when it was fixed. After all, the case turns on security claims about a system that was manifestly insecure. In effect, the plaintiffs are saying that the system was secure in all relevant respects except for one about which

P.G. 

67  
68.

they will give no further information. Yet this hidden insecurity, if revealed, is likely to narrow down substantially the suspects in the case - quite likely excluding the defendants entirely.

5. Let me give one possible explanation of what happened. The critical vulnerability becomes known to a disgruntled member of staff at Diners UK. He uses the Racal HSM to decrypt the PIN corresponding to the defendant's account, or simply to print out a PIN mailer. He makes up a card with the account details, and performs the fraud over the following weekend. He chooses an account that has been temporarily stopped in the hope that the loss will fall on Diners rather than on an innocent customer - who in the UK at least would have been likely to complain loudly and bring the matter forcefully to the attention of the police, quite possibly soon enough for the culprits to be identified from CCTV footage or from the testimony of witnesses who made subsequent transactions.

6. Here is a second possible explanation. A member of staff at SBSA has access to a machine through which transactions pass en route from Diners UK to the machine in South Africa that authorises them. Operating in collusion with a colleague who has travelled to the UK, she intercepts and manually authorises all incoming transactions directed at the plaintiff's account. Again, she chooses an account that has been temporarily stopped in the hope that the loss should fall on the plaintiff.

PL  
NB



69.

5

Such an attack was to my certain knowledge used against a South African bank in 1985, when technicians reprogrammed a communications processor so that it approved all the transactions sent in from a certain machine over a weekend. I am prevented by an obligation of confidentiality from giving further details, as I learned of this case while consulting for a South African bank in the late 1980s. In that case, the criminals manipulated authorisation responses, so it was not even necessary for the conspirators to find out the PIN on the target customer account; a transaction refused on the grounds of 'wrong PIN' would be turned into an approved transaction just as surely as a transaction refused on the grounds of 'insufficient funds' or 'daily transaction limit exceeded'. The thieves simply used stolen cards to empty the ATM. If in fact a PIN was required in the present case - of which I am not convinced - and SBSA insiders were the culprits, then it might have been obtained by abusing SBSA's cryptographic facilities.

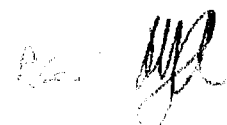
7. These are only two out of a very large number of possible attacks on the plaintiff's ATM systems that could have involved corrupt insiders, technically skilled outsiders, or both. The papers cited in section 4 of my expert notice give many more examples. At present, though, we do not know enough about the systems used by the various institutions that participated in these transactions to narrow the field down to a small number of highly likely candidates.

67.

70.

6

8. I would like to briefly mention the case R v Munden, in which I acted as an expert and to which Craig Bond is presumably referring when he states that I have used aggressive discovery before in ATM cases. John Munden was a Cambridgeshire police constable who complained about six phantom withdrawals from his account at the Halifax Building Society in September 1992. He was told that as the bank's systems were secure he must have made the transactions himself or caused them to be made. When he persisted in complaining, the Halifax had him arrested for attempting to defraud them. He was convicted at Mildenhall Magistrates' Court on 12th February 1994. Britain at that time was suffering a wave of phantom withdrawals (as it is again now). As in the present case, I was brought in as an expert halfway through the trial, and because of the Magistrates' Court rules I was not able to get any hard information on the systems used by the Halifax. All I could do was to help in the cross-examination of their expert, and respond by relating the long history of ATM frauds and the many ways in which they had been carried out. However to each of the possible attacks that I described, the expert for the Halifax flatly denied in rebuttal that that specific attack could have worked against their ATMs. The defence had thus been set an impossible burden - to guess at the vulnerabilities in a system to which we had no access, and where even a successful guess could be denied by the other side with no prospect of independent verification.



10.  
11.

7

This led to Munden's conviction, which became a cause celebre after he complained of a miscarriage of justice and obtained substantial publicity.

9. For the appeal, the complainant had a lengthy expert notice prepared by their auditors claiming that their ATM systems were secure. The defence therefore applied for, and got, an order compelling the complainant to grant to me, as the defence expert, the same access to their systems and documentation for the purposes of inspection that had been granted to the prosecution experts. The Halifax refused to comply and the court accordingly barred the prosecution from bringing any expert evidence at all. The appeal was upheld on the 8th July 1996, at Bury Crown Court. By that time, several criminals had been convicted of ATM fraud and there were further convictions during the mid-1990s, leading UK banks to abandon their policy of blanket denial that ATM fraud was even possible. The consensus of professional opinion was that the Halifax had erred disastrously by having action taken against its customer.

10. The parallels with the present case should be clear. It has already been suggested during Gibson's cross-examination (eg. transcript, p 280) that the defence cannot win its case by a number of generalities about the efficacy of systems, whether they can be hacked into and so on. My own expertise of ATM security and its failures is very much broader and deeper than Mr Gibson's, and I am the author of the main articles on the


P.S.  


12.

8

subject in the refereed scientific literature. However, should this be insufficient for the Court, then the matter might proceed as follows. I will testify that the plaintiff's broad claims of system security are insupportable. I will testify that the IBM 4758, which is similar to the 4753 and (now also) 4755 relied on by the plaintiff, is insecure and that we have demonstrated an attack. The plaintiff may then baldly claim that 'the 4753 is different' and even if this claim is likely to be immaterial or misguided, we will have no effective way to rebut it. (C Bond already has so claimed, and appears to have misunderstood the issue; I will return to this below.) I will also testify that the VISA security module, the precursor to the Racal RG7000, is vulnerable in many ways; the plaintiff's expert may simply aver that the Racal device is not vulnerable. The same scenario might be repeated over and over. The end result might be as in the Munden case: an impossibly high burden for the defence, preventing the defendants from getting a fair trial. The last similarity with Munden on which I will remark here is that I am informed that the current case is not an isolated matter.

11. I would therefore respectfully submit that the honourable Court should consider what will constitute the appropriate burden for the defence in this case, and make orders in the light of that, thereby affording the defence a proper opportunity of placing all pertinent information before this Honourable Court, which is in the interests of justice and which will

P.C. 

9

not be possible without proper disclosure by the Plaintiff and the access sought.

12. I will now pass to the examinations and tests that we wish to perform. Because of the distinct possibility that the fraud was carried out by someone working for Diners UK, we wish to demonstrate to the satisfaction of the Court that such an employee could have abused the Racal RG7000 or 7100 devices (RG) available in the UK to decrypt the PINs maintained there for Diners SA customers. If the court is satisfied with the evidence in the public domain (e.g., 4.5 and 4.6), then we need go no further. However if the defendant proposes to challenge this and say that 'the RG is not vulnerable' then we would much prefer to prove that it is indeed vulnerable and we are confident that we will be able to do that.

13. To prove the vulnerability of the RG HSM, we propose to first analyse its transaction set using the manuals sought under the rule 35(3) notice and determine which of the attacks known to us should work against it. We then propose to verify that at least one of these attacks works in practice. To do that, we will connect a personal computer to the device, pass a number of transactions to it, and analyse the results. This will simulate the kind of attack in which a bank insider programs one of the computers

PC 


74

10

to interrogate the HSM and analyse the results. I stress that we do not propose to tamper physically with the device; accordingly the risk of protective self-destruction will be no higher than in normal operations. In the case of an RG device situated at Diners UK in Farnborough, Mike Bond and I would travel to Farnborough to conduct the tests under the eye of the Diners staff there.

14. In the case of the IBM 4753 or 4755, we propose to send a set of test transactions which we used to prove the vulnerability of the later 4758 to South Africa. The test will be conducted by Mr Gibson, under my supervision, at the premises of Standard Bank. Again, we do not propose that Mr Gibson tamper physically with the device, and the tests can be conducted under the supervision of Standard Bank personnel, so there is no increase in the risk of protective self-destruction of the equipment.

15. In the case of the other equipment to which access is sought and which has not already been destroyed by the plaintiff or its associates, a similar procedure will be followed. We will analyse the documentation requested under the rule 35(3) notice, plan a series of attacks, write software to carry them out, and record the results for use in evidence. In the event that the equipment is in the UK, the tests will be performed by myself and by Mike Bond or by Richard Clayton acting under my supervision (as

P.G. 

11

well as the supervision of the equipment's owner where relevant). In the event that the equipment is in South Africa, the tests will be designed by myself, Bond and Clayton and carried out by Gibson under my supervision as well as under local supervision by the equipment owner.

16. The plaintiff has argued at several places in Craig Bond's affidavit that insofar as the examinations pertain to vulnerabilities of a generic type of equipment, rather than of the specific instances of this equipment on whose security the plaintiff relies, the defence should simply purchase samples on the open market and test them at our leisure. This is not possible, as many of the items (including the RG devices) are only sold to banks and other companies involved in transaction processing. Our attacks on the IBM 4758, for example, were designed in the abstract, on the basis of publicly available information, then tested surreptitiously using a device in the possession of one of IBM's competitors. Only once we had published the results was IBM prepared to let us have a real device to experiment with. In the case of the Racal devices, not even the manuals are available to us, despite a number of contacts with them. Without the assistance of the Court, it appears unlikely that we will be able to get either a manual for the RG series devices, or access to a device to confirm the attacks that we find.

12

17. There is also an issue of cost. Many of the systems at issue are so expensive that it would be completely impractical for the defendants to purchase examples for experimentation. A mainframe computer installation, for example, will typically cost millions of pounds. Many are proprietary, and cannot be purchased short of purchasing the company that owns them.
18. The plaintiff also argues that the state or condition of individual computers is irrelevant to our case. That is not so. The security of many of the devices in question may be severely affected by their configuration, maintenance, modification status and physical location. (This is not an exhaustive list.) The generic attacks that we have discovered on many cryptographic processors represent merely the worst case for the defence.
19. Craig Bond claims for the plaintiff in section 25 of his affidavit that neither Standard Bank nor Diners International has any spare cryptographic processors that can be tested using default keys or test keys. This claim is simply astonishing. Every bank for which I have ever consulted has spare processing facilities in case the main production facilities are rendered inoperative by a disaster such as fire or flood. Spare capacity is also required for developing and testing new systems, and so that systems can be taken down for routine maintenance. The



27.  
17.

13

most usual configuration is that a bank will have a main production site, plus a second site with similar equipment that is normally used for development and testing but which can in emergency be used to run production systems. The need for backup has been emphasised by the Bank for International Settlements for over twenty years, and has been industry standard practice since even earlier. If indeed Standard Bank has only one cryptographic processor, then presumably during annual maintenance (to replace the battery) there is a period of perhaps half an hour during which no ATM transactions can be processed; and if the processor were to break, the bank would be unable to accept ATM transactions for perhaps several weeks while a replacement device was ordered and imported. Furthermore, during the development and testing of new applications, the bank's programmers would have to use cryptographic equipment containing live keys. If Standard Bank has indeed been operating in this way, then their giving programmers and testers access to live keys provides yet another possible explanation of the frauds at the heart of this case. Even if the programmers and testers are not in fact the culprits, letting them use live cryptosystems for development and testing falls way short of industry standard practice.

20. The plaintiff argues that access to its systems would expose customer confidential data. Yet banks expose customer data to all sorts of third parties - auditors, insurance inspectors, security consultants, equipment

P. 2  
K.A.

vendors and maintenance contractors. (This list is not exhaustive.) Confidentiality is assured by laws or agreements. I cannot speak to South African law, but in the UK, it would be an offence under the Data Protection Act for me to reveal any confidential customer data learned as a result of expert witness work. I respectfully submit that it must be unusual for an expert witness to be challenged on the grounds of possible future criminal behaviour, where there is no basis set forth for such a challenge.

21. The plaintiff also argues that the design of security systems should be kept secret in the interests of security. This is an old argument and is thoroughly discredited. One of the basic principles of the engineering of cryptographic systems is the assumption that the design is already known to the opponent; thus the security of the system depends not on its obscurity, but on the choice and the subsequent protection of the cryptographic keys with which it is customised. This principle was first formally enunciated by Kerckhoffs in 'La Cryptographie Militaire' in 1883, and its wisdom has been reinforced by long experience since. In the banking world it is particularly imprudent to hope that designs will remain secret. There are some 20,000 banks issuing ATM cards, most of them using similar systems. Some of the banks are controlled by criminals, and in any case there are perhaps a million people worldwide with access to equipment such as that which forms the subject of this


78.  
M.  
78.  
  
P.S.  
M

78.  
79.

15

hearing. Denying security researchers access to product information (as **Racal** does) does not assist security; it is surely a measure aimed at limiting legal liability. Granting access to security researchers (as **IBM** does; the 4758 manuals are available on their website) is better for security. We found an attack; we reported it to **IBM**; and they fixed the problem by means of a software release. **IBM** got a more secure product, and we got the reputational benefit of several scientific papers describing our attacks and various defences against them.

22. The appropriate protection of commercial confidentiality in such a circumstance is that a researcher discovering a security flaw should hold off publication for a period of time so that the vendor can devise a fix and ship it to its customers. For example, we have an agreement with **IBM** under which we give them three months' notice in advance of publishing any information on vulnerabilities that we find, and we have no objection to entering into a similar agreement with other equipment vendors to whose equipment we have access. Such an agreement is not really necessary, since for reasons of professional ethics we would give the vendor a grace period anyway. However, for the avoidance of doubt, I have no objection to the Court imposing a suitable confidentiality condition (by which I mean one that would not burden our unrelated research work).


PC 

71.  
80.

16

23. I would point out further that I have consulted for Nedperm and for First National Bank, and that Gibson spent 13 years in the South African banking industry. It would be quite unreasonable, I respectfully suggest, for the Court to rule that we are unfit persons to have access to banking systems, when the interests of justice demand it.

24. I would further point out that Mr Lane brandished the manual of a security module in the Court during his cross-examination of Mr Gibson (transcript, p 287-8). Yet on being served a rule 35(3) notice for access to this manual and those for the other machines on whose security the plaintiff's case depends, Riccardo Jefferies says under oath that 'The plaintiff is not in possession of any of these documents' and at 3.1 'has no knowledge in relation thereto'. Yet the plaintiff's expert notices were prepared with evident knowledge of this material. Jefferies goes on to say that the plaintiff has no control over Standard Bank of South Africa Limited, yet Mr. Lane informed this Honourable Court that the Standard Bank holds the franchise for Diners Club and acts as its agent in generating all the PINs for Diners Club (transcript p 17). The plaintiff also relies on its contract with Diners International (C Bond section 12) but simultaneously claims that its contract with Diners International is too confidential to disclose (Jefferies 4.4).

PL  



80.

81.

17

25. It seems that the plaintiff has no difficulty obtaining information from Standard Bank, or for that matter from any of the overseas institutions involved in the transactions under dispute, when that information is helpful to its case. Yet when information is requested that is likely to be destructive of its case, the plaintiff hides behind technicalities. It is my own experience that banks cooperate fully when it comes to investigating fraud, and that a sincere request from one bank to another for access to information will almost always be honoured. I therefore suggest that Mr Jefferies' statement that the plaintiff has no 'ability to compel such companies to make their documentation available to defendants' is pure sophistry. If the Court were to grant a suitable order compelling the Plaintiff to furnish access to information, documents and equipment it obviously relies upon, then I have no doubt at all that the plaintiff could and would obtain access to the required information, documents and equipment without significant delay.

26. Having dealt with the need for further particulars, for documentation and for access to equipment, and with the specific objections raised by the plaintiff to access, I will now deal briefly with the criticisms raised by the plaintiff of my expert notice. Given the time pressure, this reply is inevitably somewhat perfunctory, and I apologise for this.

P.C. 

82

18


27. I note that C. Bond (who appears to attempt to try and discredit my opinions) does not claim to have any expertise in computing or any knowledge of systems analysis, security engineering, computer equipment or software. This may explain why there are many places in which my expert notice is misinterpreted. For example, in paragraph 22 page 14 I point out Bonfrer's inaccurate description of CVV encryption, in order to undermine his claim to expertise in cryptography on which the plaintiff relies. This is misrepresented by C Bond at section 16.1 page 11 as a claim that I am not 'criticising the relevance' of the IBM 2620. As a matter of fact, my notice states in paragraph 22 that I will take exception to Bonfrer's notice on numerous points, only two of which are given for brevity. The security of the 2620 and the key material it protects is germane to the case, as the inappropriate disclosure of such key material will facilitate the forgery of credit cards.

28. In sections 18 and 26, C Bond claims that the 4758 is not a successor to the 4753 but to the 4755. Again, this shows a misunderstanding perhaps deliberate - of the attacks disclosed in our published papers, and of the open literature, specifically IBM Systems Journal v 30 no 2 (1991), which describes the IBM product range of that era. The attacks that we developed utilise flaws in the CCA software that runs on top of a platform, which was available in the early 1990s as the 4753 or 4755 or

P.E. 

the ICRF, depending on the packaging and on the transaction throughput supported. The 4758 is the modern, higher-performance platform on which the modern version of the CCA software runs. It is certified to FIPS 140-1 level 4, so there is no reason why it should be encased in a further tamper-resistant enclosure. Assuming that one of our attacks still works on the earlier versions of CCA - and I can see no reason why it would not, as we exploited application-level design features and backwards-compatibility features in different attacks - then there is no reason why physical penetration of the 4753 would be required. That was never the relevant vulnerability.

29. In section 23, C Bond argues that intermediaries such as Link, TNS and Diners UK could not possibly have been responsible for the fraud, and therefore our request for information concerning them is in bad faith. I explained above how an insider at Diners UK could have easily caused the fraud had he been able to abuse the Racal HSM to decrypt the defendant's PIN. An insider at Diners UK could also have used a misconfiguration of an upstream system to perpetrate the fraud. For example, the integrity and authenticity of transaction messages flowing between intermediaries is in theory assured by computing Message Authentication Codes (MACs) on them. However, in practice, this precaution is often dropped for performance reasons. If TNS did not verify MACs on all the authorisation response messages coming from

P.G. 

83

Diners UK, then a programmer at Diners UK could have subverted the network so that all authorisation request messages relating to the defendant's account were met with a positive authorisation response, regardless of whether the PIN was correct or not. As I remarked above, such a fraud actually occurred in South Africa in the 1980s.

30. In section 28, C Bond claims that I do not explain the basis for my belief that the two most likely causes of the frauds were one or more insiders at Diners, and one or more insiders at Standard. This is simply untrue. The reasons for my preliminary opinion are developed throughout my expert summary, and set out concisely in sections 44-52.

31. In section 28.6, C Bond claims that the PINs are not stored in the United Kingdom at all. This is in clear conflict with the expert notice of Bonfrer (especially sections 74 et seq.), according to which Diners UK stores encrypted PINs under local master key variants and uses them to authenticate incoming transactions. The Racal devices perform the necessary decryption. If they are similar to the other security modules of which I have experience, it will also be possible to use them to print out PIN mailers. Thus even if there is no technical attack at all on the Racal device, in the sense that it functions exactly as its designers intended, it is quite possible that an insider can abuse an authorised function - PIN

*[Handwritten signature]*

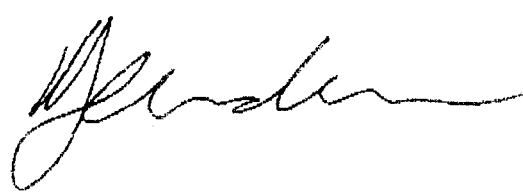


85


printing - in order to access the PIN of a South African customer at  
Diners in Farnborough.

32. On the basis of the above, I respectfully submit that the defence be  
granted further particulars as sought of the systems on whose security  
the case turns, together with the documents and access to equipment as  
requested. I further respectfully submit that any bad faith in this matter  
lies on the side of the plaintiff, in view of the lengths to which they have  
gone to deny the defence access to the information needed for a fair  
trial.

DEPONENT



I certify that the Deponent has acknowledged that he knows and understands  
the contents of this Affidavit, which was signed and sworn to before me this  
~~17th~~ <sup>20th</sup> day of ~~June~~ <sup>September</sup>, the regulations pertaining to the commissioning of such  
Affidavits having been complied with.

P.L. 

P.L.

85

COMMISSIONER OF OATHS P. GITTINS

FULL NAME: PAUL GITTINS

BUSINESS ADDRESS:

KING & CO (SOLICITORS)  
ST. ANDREWS HOUSE  
59 ST. ANDREWS STREET  
CAMBRIDGE  
CB2 3DD

IN THE HIGH COURT OF SOUTH AFRICA  
(DURBAN AND COAST LOCAL DIVISION)

87

Case No: 00/3156

In the matter between:

DINERS CLUB (SA) (PTY) LIMITED

Plaintiff

and

SINGH, ANIL

First Defendant

SINGH, VANITHA

Second Defendant

---

FILING SHEET - PLAINTIFF'S REPLYING AFFIDAVIT

---

Presented for service and filing by :

Dated at JOHANNESBURG on this the 25 day of SEPTEMBER 2002.

---

(Sgd.) A. S. L. TURNER**BOWES & TURNER Inc**  
Plaintiff's Attorneys  
c/o **GOODRICKES**  
28<sup>th</sup> Floor  
320 West Street  
DURBAN  
Tel: (031) 301-6211  
Ref: Mr J A AllanTO:  
THE REGISTRAR  
THE HIGH COURT  
PIETERMARITZBURG

AND TO:  
**J KISSOON SINGH INC**  
Defendants' Attorneys  
First Floor  
International Plaza  
128/132 Commercial Road  
DURBAN  
Ref: Ms Patel/sb/03S944K01

88

Received a copy hereof this day of  
September 2002

---

For: DEFENDANTS' ATTORNEYS

ASTred25 902  
C:\SUP\DI2518 AFF CB

**COPY 89**

**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 REPLYING AFFIDAVIT**

---

I, the undersigned,

**CRAIG BOND**

do hereby make oath and say:

- 1 I am a director of the Plaintiff and the facts herein contained are within my personal knowledge save where otherwise stated or appears.

*P.B. 8*

2 I have read the affidavit of Anil Singh and wish to reply thereto as more fully hereinafter set out.

3 AD PARAGRAPHS 3 AND 4

I note the averments herein.

4 AD PARAGRAPHS 5, 6.1, 6.2, 6.3, 6.4 and 6.5

4.1. I am advised that the expressed intention of serving a Rule 36(6) Notice was made more than simply "*in passing*" and was sufficient to provoke a response from the Plaintiff's senior counsel.

4.2. Be that as it may, what is significant and remains unexplained, is why the Defendants waited until the 27<sup>th</sup> August 2002 to serve the Notice. Indeed, in paragraph 8.4 of the affidavit deposed to on the 17<sup>th</sup> June 2002 by Dr Anderson in support of the application for leave to take his evidence on commission, he stated: *'I have advised the legal representatives of the Defendants as to additional information, documentation and access to equipment which is necessary for me to be able to properly prepare for my evidence and to demonstrate to this Honourable Court the vulnerabilities in*

P.B.

*the proposed testimony of the Plaintiff's witnesses. I understand that as a result, a request for particulars for trial, a notice for better discovery and a notice to make equipment available for inspection will be delivered."*

- 4.3. It is accordingly incorrect to say that Dr Anderson was only able to "properly apply his mind to what information ought to be requested, what additional documents ought to be discovered by the Plaintiff and what equipment ought to be requested for inspection during August 2002." That advice had already been given prior to the 17<sup>th</sup> June 2002.
- 4.4. This application could certainly not have been moved during February 2003 without the consequence that the commission and the continued hearing would be placed in jeopardy.
- 4.5. The Rule 35(3) Notice has been responded to and as stated by the Defendants a Rule 30 Notice has been served in relation to the request for particulars. The Plaintiff has not sought to have the Rule 30 determined in these proceedings as it is, I am advised, a point of law which could be determined by any Judge. Either the rules allow the service of a request for particulars for trial during the course of the trial or they do not. The only issue which

PBK

concerned the Plaintiff was the Rule 36(6) Notice and the application was brought to have same determined as a matter of urgency before the Honourable Mr Justice Levinsohn. The mere fact that the Defendants are *dominus litis* in serving the notices does not deprive, I am advised, the Plaintiff of its entitlement to relief and to take such steps as would ensure that the trial be expeditiously brought to a conclusion.

- 4.6. It is quite inappropriate for the Defendants to have raised the question of the negotiations which ensued between the parties. It is accordingly necessary for me to set the background to such negotiations. An investigator from The Standard Bank of SA Limited had, per chance, received evidence from an informer as to the manner in which fraud was perpetrated in relation to ATM transactions conducted overseas. An interview with her had been recorded on a video tape which was shown to the Plaintiff's legal representatives. The Defendants' counsel were invited to view the video tape which was shown to them by the investigator in order that they be properly informed so as to give the Defendants appropriate advice. The suggestion to the Defendants was not whether they "*would be prepared to enter into negotiations for a settlement of the dispute*" but rather given the information at hand, they ought to settle the matter. The Plaintiff is not in possession of

LB



93

5

the tape and is not able to identify the informant. Since then further information has come to hand and the Scorpions are investigating same.

5 AD PARAGRAPHS 6.6 to 6.11

- 5.1. I am advised that Rule 21 does not enable a party to litigation to deliver a notice requesting further particulars after the trial has commenced. The request for particulars must be served not less than twenty days before trial.
- 5.2. The trial in this matter commenced on the 4<sup>th</sup> March 2002 and the request for particulars was served on the 27<sup>th</sup> August 2002. It clearly constitutes notice in terms of Rule 21 and for that reason, I am advised, a notice in terms of Rule 30 was served on the Defendants' attorneys.
- 5.3. I do not understand on what basis, having served the request for particulars for the purposes of trial out of time, the Defendants can now seek an order authorising or condoning the delivery of the request or granting permission to deliver such a request. The Rules simply, I am advised, do not contemplate the requesting of particulars during the course of a trial. The purpose of a request

RB

for particulars is to prepare for the trial and not during the trial. What in fact the Defendants are seeking is for this Honourable Court to establish a new rule altogether which I am advised is inappropriate.

5.4. The Defendants have been aware since the commencement of this litigation that, if they were to challenge the fact that the First Defendant's PAN and PIN were utilised for the transactions in the United Kingdom on the 4<sup>th</sup> and 5<sup>th</sup> March 2000, they would require the services of an expert. They waited until very late in the day to employ the services of Gibson and only after Gibson had given evidence did they then start looking for another expert. They should have done this earlier and would have, I have no doubt, come across Dr Anderson. It is accordingly no excuse to say that they are only now receiving expert advice.

5.5. As one would anticipate the request for the purposes of trial does not arise out of the pleadings but constitutes a long list of interrogatories in relation to issues in which, I am advised, the Plaintiff bears no evidential onus. For instance the questions raised in paragraphs 1 to 11 were canvassed in the evidence of Du Preez in the cross-examination of her by Defendants' senior counsel as emerges, for example, from pages 59 to 62 of the Record. This

has always been an issue and was even foreshadowed by requests made by the Defendants at the pre-trial conference. Consequently they did not need Dr Anderson to advise them thereon.

- 5.6. The issues raised in paragraphs 12 to 17 are again nothing new in these proceedings as it has always been the Defendants' case that the number of transactions *per sé* demonstrated a vulnerability in the system. Quite clearly they did not need Dr Anderson to advise them thereon as is evidenced by the testimony of Gibson who also made reference thereto.
- 5.7. Paragraphs 18 to 24 of the request again do not arise out of any technical input by any of the experts. These are factual issues which frankly could have been requested prior to the commencement of the trial and have nothing to do with the state or operation of the computer systems and whether these computer systems are vulnerable.
- 5.8. It is inadequate for the Defendants simply to say that they require the information without explaining precisely why the information is required, establishing an entitlement thereto and giving an adequate reason for not having asked the questions when they ought to have, namely prior to the commencement of the trial.

6 AD PARAGRAPHS 6.12 and 6.15

6.1. The Defendants must have been well aware of the reason for short notice being given to them as to the nature of the examination which they wished to conduct of the various computer systems. It was not of the Plaintiff's making that the notice in terms of Rule 36(6) was only served on the 27<sup>th</sup> August 2002. The Defendants had already been advised by Dr Anderson, at latest by the 17<sup>th</sup> June 2002, that he required the identified computers to be subjected to examination. It was accordingly necessary to put the Defendants on short notice in order to establish same and in particular whether the fears that the computer systems would be compromised or could be destroyed in the process were in fact a reality. All of this had to be done in sufficient time in order to put an application before his Lordship Mr Justice Levisohn prior to him taking his sabbatical.

6.2. It is not correct that, had the Defendants withdrawn the notice, as was demanded in that letter, an application would be brought. The request for information regarding the examination was incidental and only significant insofar as the Plaintiff did not withdraw the

BB/A

notice. It was only after the time period prescribed in that letter had elapsed that the Plaintiff brought the application.

- 6.3. I am advised that it is incumbent upon a party giving such a notice to advise of the nature of the examination and that the proposition that *"all the Plaintiff had to do was to decline to submit the items requested to the inspections"* is not correct.
- 6.4. According to the application brought by the Defendants for leave to take evidence on commission consultations were held with Dr Anderson on the 2<sup>nd</sup> and 3<sup>rd</sup> June 2002. He was able as a result thereof to advise the legal representatives as to what equipment he wanted to examine and stated categorically in paragraph 8.3 thereof that he anticipates *"that Bond and Clayton can effect a rapid and concrete demonstration to this Honourable Court of the insecurity of the IBM 4753 and RACAL RG 7000 hardware security modules."* However, he added, that *"the equipment they will use to do this, and which is available at the computer laboratory, could not be exported from the United Kingdom without a license that is unlikely to be granted quickly, or indeed at all on terms that the University will find acceptable."*

PJB  
AS

6.5. In the result it would seem that Dr Anderson had already advised the Defendants as to the examination which he wished to subject the computer systems to and it would have been a simple matter for a telephonic consultation to have taken place in order to clarify any doubts which the Defendants might have had. Bearing in mind that a notice in terms of Rule 36(6) I am advised, requires that the equipment must be made available for inspection for ten days from the date of service of the notice, five working days to provide the information is hardly unreasonable.

7 AD PARAGRAPH 6.13

I simply do not understand the Defendants' submission.

8 AD PARAGRAPH 6.14

8.1. I reiterate what has been said in the founding affidavit.

8.2. I fail to see the relevance of the Plaintiff's counsel having put the content of the various expert summaries of the Plaintiff's experts to Gibson. I am advised that it is proper to have done so regardless of whether that evidence is lead in rebuttal.

BB

9 AD PARAGRAPHS 6.16 AND 6.17

I shall deal with the affidavit filed by Dr Anderson separately.

10 AD PARAGRAPH 7

I reiterate what is stated in the founding affidavit.

11 AD PARAGRAPH 8

The Plaintiff will not object to the filing and use of a facsimile of the affidavit.

12 AD PARAGRAPH 9

12.1. Whilst it is correct that the Plaintiff sought and obtained an order for the hearing of evidence on commission it does not, of necessity, mean that such evidence would in fact have been taken on commission if rebuttal evidence was not necessary. Furthermore, even if the Defendants adduce evidence of their experts it still does not compel the Plaintiff to lead any evidence of its experts on commission or at all.

LB

12.2. The simple proposition is that the Defendants are not entitled to rely upon being able to cross-examine these witnesses as it bears an evidential onus to relieve it of the consequences of the *prima facie* evidence against them.

12.3. I am advised that the Defendants have misinterpreted the rule and that appropriate argument will be addressed in this regard.

### **AD THE AFFIDAVIT OF DR ANDERSON**

#### 13 AD PARAGRAPH 4

13.1. I assume that Dr Anderson has read the record of evidence and the cross-examination of Du Preez where it was explained that there was no limit in relation to a Diners Club Card on the number of transactions in any given day per card. The only limit was the amount which could be withdrawn in relation to each transaction. This is a feature of the Diners Club system and it is inappropriate to compare that system with the operation of any other accredited card which might have a limit on the number of daily withdrawals or the total amount which could be withdrawn in any given day.

12/5/82



13.2. It would seem that Dr Anderson is confusing the facts of the case with whether the system is secure and it is interesting to note that he does not point to a single piece of equipment or computer system which has to be examined in this regard.

#### 14 AD PARAGRAPH 5

14.1. Again Dr Anderson has not acquainted himself with the facts "*Diners UK*" (whatever he means by this, the position had been explained in the founding affidavit) is unable to access the PIN which is not stored in the United Kingdom but in Germany and cannot print out a PIN mailer. In order to do so the person would have to have the PIN Master Key (PMK). Dr Anderson assumes that the PMK is transported outside of The Standard Bank of SA Ltd and it is not.

14.2. "*Diners UK*" cannot access the PAN and cannot do it by reference to the name of one of Plaintiff's customers.

14.3. Nobody in the United Kingdom would have known that the First Defendant's domestic ATM operations had been suspended.

RB

14.4. Dr Anderson clearly has not read the record carefully as it was put to the First Defendant in cross-examination that the Diners Club card could be used overseas and that the block put on his card only affected domestic ATM transactions and not transactions abroad (Record p184). His example is accordingly inapposite.

14.5. Furthermore, the First Defendant's card would only have been suspended for ATM transactions 30 days after his statement of account dated 1<sup>st</sup> February 2000 (as per B7 to the Particulars of Claim: p26) should have been paid. On the facts of this matter it would only have been on the 2<sup>nd</sup> March 2000.

14.6. What is significant is that Dr Anderson is not able to point to a single attack on the RACALS or IBM 4753/4755 which was successful whilst the computers were in operation. RACAL and IBM know of no successful attacks. For such an attack to have worked the person would have to have had the HSM in an authorised state which would mean breaking the Local Master Key (LMK) which is randomly created in TDES. Gibson has conceded that this never happened.

15 AD PARAGRAPH 6

15.1. Yet again it would seem that Dr Anderson has not carefully read the expert summaries filed on behalf of the Plaintiff. The transactions do not pass through the computer system of The Standard Bank of SA Ltd en route from "Diners UK" to South Africa and there is no authorisation done in South Africa for such ATM transactions.

15.2. I cannot comment on the general statements he makes in relation to an incident in the late 1980's but would suggest that, even on Dr Anderson's showing, the whole process of PIN management has changed substantially since then in relation to both the hardware and the software. A simple statement that thieves use stolen cards is of really no interest in this matter as the First Defendant's card was not stolen.

15.3. It is interesting to note that Dr Anderson for the first time in this affidavit challenges whether a PIN was required in the present case. Gibson, on the other hand, has contended that it was. Furthermore in Dr Anderson's expert summary he does not challenge any of the Plaintiff's experts in this regard. If, however, he does actually believe that a PIN is not necessary then one wonders why he wishes to examine any of the cryptographic equipment.

103

## 16 AD PARAGRAPH 7

16.1. Dr Anderson has now had a number of occasions to examine the probabilities of the case in order to put forward a theory which contemplates the probabilities and the facts of this matter. It is clear, both having regard to his expert summary and to his two latest theories which I have dealt with previously, that he still has not acquainted himself with the facts. A process of speculation can hardly assist this Honourable Court in coming to a conclusion where the basis of such speculation is remote from the facts and the probabilities.

16.2. Dr Anderson does not disclose what information is lacking. A very full description of the computer systems, the functions and operation is contained in the Plaintiff's expert summaries.

## 17 AD PARAGRAPHS 8 AND 9

17.1. I fail to see the relevance of the Halifax Building Society case. It was, first of all, a criminal prosecution of which the Halifax Building Society was the complainant. The Building Society refused to allow its security to be compromised by the defence and it was this

PB

refusal per sé that lead to the dismissal. There is no indication that the integrity of the computer system in use by Halifax was tested evidentially or was the subject of any finding by the Crown Court.

17.2. Again, however, one is confronted by broad generalisations made by Dr Anderson in relation to "phantom withdrawals" and certainly he has established no basis for the admission, I am advised, of other incidences. There are certainly different facts in those cases and there is no suggestion as to what systems were utilised in relation to those transactions.

17.3. Dr Anderson is unable to give any examples of the RACALS or IBM 4753/4755 HSMs being successfully attacked whilst in operation in a commercial environment.

#### 18 AD PARAGARPH 10

18.1. I fail to see what parallels there are between the present matter and that of the Halifax matter.

18.2. It is not clear to me the point that Dr Anderson is making. Is the suggestion that this Honourable Court should simply accept his expertise because his experience is "much broader and deeper than

BB

Mr Gibson's" and because he is "the author of the main articles on the subject" and, if this is the case, he will not then give the evidence?

- 18.3. What, however, emerges from the evidence that he says that he will give is that he does not need access to any of the computers which he wishes to examine in order to express his views.
- 18.4. As was pointed out in the founding affidavit the IBM 4753 is the HSM which houses the 4755 which is a cryptographic adaptor card. The Plaintiff does not baldly claim that the 4753 is different but only that the 4753 is not the precursor to the 4758 as suggested by Anderson. It is then a very simple matter for the Defendants to demonstrate, if they can, that in fact what Dr Anderson says in his summary is correct namely that the IBM 4753 was the precursor to the IBM 4758. One can imagine a number of ways of effectively rebutting Plaintiff's evidence as it is simply a question of fact. It is a fact which can be ascertained from IBM without any difficulty whatsoever.
- 18.5. Again I do not understand Dr Anderson's view in relation to the RACAL RG 7000. The expert summary of Bond is to the effect that the RG 7000 was susceptible to an attack but that it had been

BB

corrected. Accordingly the question is not whether the RACAL RG 7000 is subject to attack but whether, at the time of the transactions, the software had been updated.

18.6. It is again significant that Dr Anderson deliberately moves away from the facts and does not answer, as he cannot, the question why any of the RACAL HSM's are relevant and consequently, yet again, his hypothesis resides only in a vacuum.

18.7. It appears that Dr Anderson has been given other information which he does not disclose when he alleges that this matter is not isolated. He is correct, and I annex hereto marked "R1" a copy of an affidavit deposed to by RAMESH SINGH on the 7<sup>th</sup> August 2002 in which he admits to committing a fraud. It involved the Plaintiff, the same ATMs were used and the PIN was sought to be issued only shortly before the transactions took place in London.

19 AD PARAGRAPH 11

I am advised that the test of the "*appropriate burden*" is inapposite and that appropriate argument will be addressed at the hearing hereof.

20 AD PARAGRAPH 12

PB

20.1. It is extraordinary that, having spelt out in detail to Dr Anderson the facts of this matter, namely, that the RACAL HSM's could not have been attacked and the First Defendant's PIN divulged simply because the First Defendant's PIN only passed through them subsequent to the first transaction taking place, he makes no attempt whatsoever to demonstrate to this Honourable Court what the relevance is of the experiment which he wishes to subject the RACALS to.

20.2. The PIN is not maintained in the United Kingdom and "Diners UK" cannot from its offices in Farnborough access the PIN. There is network security in place. The RACALS in the United Kingdom which he wishes to examine are merely translators i.e. they pass the information on.

#### 21 AD PARAGRAPHS 13 AND 14

21.1. Dr Anderson has been given ample opportunity to apply his mind to the facts and neglects to do so. He simply does not explain the relevancy of the RACALS.

21.2. The examination which Dr Anderson proposes is, in itself, irrelevant. As mentioned earlier, the HSMs have to be in an

BB



authorised state. A person wishing to extract information would have to have broken the LMK's which nobody has successfully done. Accordingly, what Dr Anderson is suggesting is that the HSMs be given to him in an authorised state or that the HSMs are shut down and taken off line. In either case, the experiment does not emulate what had to have happened, on his theory, and accordingly, even if the experiment was successful, does not prove that a person in the employ of one of the organisations could access the information.

21.3. If the suggestion should be made that this fraudulent person had access to the HSMs in an authorised state, the simple answer is that it could not have happened as it requires the coincidence of two smart cards or passwords held by different people and the transactions would be logged.

21.4. Dr Anderson's approach does highlight, however, the consequence of his experiment. The shutting down of the HSMs would mean that as long as they were being experimented on no transactions will take place. All transactions will stop altogether. The computer systems have back-ups for the very reason that it is necessary to guard against a computer going down. Consequently the risk of

PJB

having no back-up whilst Dr Anderson and his associates experiment is not one which can or will be taken.

21.5. For the same reason as I have stated previously there is no relevance of experimenting with back-up equipment as it will not show how the person was able to break the LMK. The back-up unit is as much part of the system as the production unit and neither The Standard Bank of SA Ltd nor Diners Club International Ltd, its subsidiaries or associated companies will allow them to be experimented on.

21.6. The Defendants have not sought to examine the IBM 4755 and as we understand Dr Anderson he takes issue with Bond that the 4755 was the precursor to the 4758. One would have thought that it would have been a simple exercise for Dr Anderson to have established whether he or the Plaintiff is correct in relation to this.

## 22 AD PARAGRAPH 15

22.1. It is again extraordinary that Dr Anderson has not addressed specifically which equipment he is referring to. The Plaintiff has been at pains to indicate what equipment is extant and what is no longer in use or available for examination. A bald statement that

110



they intend to use "a similar procedure" tells one nothing as to what examination they intend to conduct in relation to that equipment or even, for that matter, address the relevance of the particular piece of equipment with regard to the facts of this case.

22.2. Dr Anderson's approach to the matter is demonstrated by the use of words such as "destroyed" suggesting that the respective parties actually and intentionally "destroyed" the equipment. This is simply not correct and is inflationary.

#### 23 AD PARAGARPH 16

23.1. I do not understand Dr Anderson's views in this regard. It would seem that what he expects is that the Plaintiff who is not in control and possession of any of the computer systems which he wishes to examine, if it cannot persuade The Standard Bank of SA Ltd or Diners Club International Ltd, its associates or subsidiaries to provide the equipment, to purchase the computer systems in order to facilitate his tests. The unreasonableness of his attitude is highlighted by the fact that not even now for the purposes of this application has he addressed his mind to the probabilities which are prevalent in this case as distinct from a purely hypothetical attack against various computer systems which cannot affect the outcome

of the case. Employees of those companies that possess and control those systems are maligned by him without there being any probable foundation in respect thereof.

23.2. It is also clear from the expert summaries filed on behalf of Dr Anderson, Clayton and MK Bond that indeed the RACAL, for instance, as well as the VISA HSM and IBM products must have previously been made available to them for testing otherwise it is difficult to conceive on what basis they make the comments they have. Indeed, Dr Anderson concedes that he is able to acquire equipment from IBM.

23.3. It is interesting, however, that it would seem that Dr Anderson and the Defendants have made no attempt whatsoever to obtain the computers in question for the purposes of his experiments.

23.4. Dr Anderson does not disclose anywhere why he needs the mainframe computers or what experiments he intends to conduct on them. In order for his experiment to have any relevance he would first of all have to breach the security which protects the systems. In the case of The Standard Bank of SA Ltd this would mean breaking "Top Secret" and "SOBR". Dr Anderson does not suggest that he can do this.

BB

23.5. One of the fundamental mistakes that Dr Anderson makes is that he treats individual components of the system in isolation. Whereas it is the working of the systems in their entirety that is significant. There are security systems in place which protect the operation of the systems and prevent the sort of attack that Dr Anderson is suggesting might be successful.

#### 24 AD PARAGRAPH 17

24.1. Anderson highlights one of the very difficulties with which the Plaintiff is confronted. Whilst it is correct that the systems employed are very expensive, Anderson would, nevertheless, have The Standard Bank of SA Ltd and Diners Club International Limited, its subsidiaries or associated companies make same available to him and his associates so that he can experiment therewith in an attempt to explain theories which are completely divorced from the probabilities of this particular case.

24.2. This paragraph shows Dr Anderson's intent, namely experimentation, which he will carry out in the hope that it will provide some explanation for the ATM transactions forming the

BB

114

subject matter of this action. I again refer to what I have said previously.

#### 25 AD PARAGRAPH 18

25.1. Clearly, Dr Anderson has misunderstood what has been said in the founding affidavit. The state or condition of most of the equipment on the facts of this matter is irrelevant. I reiterate that there is no suggestion that the components to the system were not working and consequently the state or condition of that equipment is not in issue. The question is only whether a generic attack on the items will succeed.

25.2. Furthermore it seems now that beyond examining the particular items in question Dr Anderson wants to consider holistically the access control and management of these computer systems which has not been and cannot be asked for in terms of the Rule 36(6) Notice. No one person has or will ever be given end-to-end access to the various computer systems for obvious reasons.

25.3. I do not understand the last sentence in this paragraph.

#### 26 AD PARAGRAPH 19

P.B.

26.1. It is correct that neither The Standard Bank of SA Ltd nor Diners Club International Ltd has "spare cryptographic processors". There are back-up systems, providing test and disaster facilities, which are part of the operating systems of the Bank and Diners Club International Ltd and cannot simply be hived off so that they can be experimented on by Dr Anderson and his associates.

26.2. If the production system goes down the back-up system must be immediately available.

#### 27 AD PARAGRAPH 20

27.1. It is clear that Dr Anderson is not a banker and simply does not have the requisite knowledge to make the statements that he makes. The Bankers in South Africa and in the United Kingdom have adopted a Code of Banking Practice which, I am advised, is consistent with the legal requirement that the Bank preserve their clients' confidentiality. It is not a question whether he is prepared to keep information confidential but the obligation which the Bank owes its customers.

RB

27.2. The Data Protection Act is not applicable to South Africa and the equipment which Dr Anderson wishes to examine in the United Kingdom is, in any event, irrelevant on the facts of this case.

27.3. An order by this Honourable Court requiring Dr Anderson not to disclose any information would not be effective as he is resident in the United Kingdom and has indicated that he will not come to South Africa.

#### 28 AD PARAGRAPH 21

28.1. The non-disclosure of information concerning the design of the products has not been discredited. Once information of this nature enters the public domain it is much easier for a would-be criminal to devise schemes to abuse it.

28.2. IBM and RACAL do their own research and development and do not need to rely upon the likes of Dr Anderson to assist them.

#### 29 AD PARAGRAPHS 22 AND 23

I fail to see the relevance of the suggestions he is making here.

EB



## 30. AD PARAGRAPH 24

- 30.1. The Record at page 287 is incorrect. Reference was made to a page out of the RG 7000 manual and not to "IG 75". One would have assumed that a person purporting to have the expertise of Dr Anderson would realise that there had been a mistake and have made the necessary enquiries. The page of the manual was given to Lane by Bonfrer during cross-examination of Gibson, and is not a manual which is in the Plaintiff's possession.
- 30.2. Unfortunately Lane did not have the correct information at hand in relation to the franchise. The Standard Bank Ltd has never held the franchise for Diners Club. The franchise has always been held by Diners Club SA (Pty) Ltd. In this regard I annex hereto marked "R2" a copy of the first page of the first Franchise Agreement concluded between the Plaintiff and Diners Club International Ltd.
- 30.3. There has never been a dispute that The Standard Bank of SA Ltd generates and issues the PINs for Diners Club SA (Pty) Ltd but it is not an agent in the strict sense of the word. It acts independently and provides a service for Diners Club SA (Pty) Ltd.

BB

30.4. The Defendants have at no stage disclosed what the relevance is of the Diners Club Franchise Agreement. Not even in this application has such relevance been disclosed and one cannot imagine how it would assist Dr Anderson in his testimony.

### 31 AD PARAGRAPH 25

31.1. The Plaintiff has had extreme difficulty in obtaining information from The Standard Bank of SA Ltd and Diners Club International Ltd, its subsidiaries and associated companies particularly where such information is of a confidential nature or might in any way compromise the security of the various institutions.

31.2. It is one thing, however, to obtain information which does not compromise security its altogether another to require a Bank or credit card institution to make its computers available for an examination which would or could compromise its security.

31.3. I know of no incident where one Bank has successfully asked another Bank to allow its computer systems to be subjected, end-to-end, to an examination and it is extraordinary that Dr Anderson suggests baldly that it has happened without giving any concrete examples thereof. In fact in the only example quoted by Dr

BB

Anderson, the Halifax Building Society was prepared to allow the criminal case to be dismissed rather than supply confidential information which would have compromised its security.

31.4. The Plaintiff is unable to make available for examination or experimentation any systems which are owned or controlled by third parties. It certainly cannot compel The Standard Bank of SA Ltd or Diners Club International Ltd, its subsidiaries or associated companies, to open their systems for the Defendants' experts in an action to which they are not parties.

### 32 AD PARAGRAPH 26

It is significant that Anderson has not dealt with the need for further particulars or documentation whatsoever which, as stated previously, having regard to the request for particulars, cannot arise out of anything that he might require.

### 33 AD PARAGRAPH 27

33.1. In the light of the allegation that the 2620 is irrelevant Anderson does not take this Court into his confidence in establishing why he suggests that the 2620 is indeed relevant. Furthermore, he does

218  
16/11

not heed the fact that the 2620 is no longer available for inspection.

33.2. The 2620 has nothing to do with the issue or generation of a PIN.

33.3. Whilst it is correct that an inappropriate disclosure of the key material facilitates forgery of credit cards, this is only relevant to point of sale transactions. This matter does not concern point of sale transactions.

#### 34 AD PARAGRAPH 28

Dr Anderson attempts to side-step the issue. Either the 4755 was the forerunner to the 4758 or it was not and that would be a simple fact for him to establish.

#### 35 AD PARAGRAPH 29

35.1. Anderson has not applied his mind to the facts. There is a fundamental basis upon which the criticism was made namely, whether upstream or downstream, the PIN and PAN never entered the systems of LINK, TNS and "Diners UK" before the first transaction took place.

LB

35.2. Conducting experiments on the computer systems will not, even on Dr Anderson's version, in any way contribute to the opinion he expressed in relation to MAC verification. It is a matter of fact, either it was done or it was not.

36 AD PARAGRAPH 30

Dr Anderson has again demonstrated in this affidavit that the basis for his belief is suspect.

37 AD PARAGRAPH 31

Bonfrer does not state that the PINs are stored in the United Kingdom. However, as a matter of fact, the PINs are stored in Germany and not in the United Kingdom. Diners Club UK Ltd is an entirely different company to Diners Club International Service Centre.

38 AD PARAGRAPH 32

Again Dr Anderson has demonstrated that he lacks objectivity and independence, both of which qualities this Honourable Court will take into

LB  
A

34 **122**

account in assessing the extent to which his testimony will assist in coming to a just and proper determination of the matter.

39 In the circumstances the Plaintiff persists in its prayer for relief.

*[Handwritten Signature]*  
\_\_\_\_\_  
**DEPONENT**

THUS SIGNED and SWORN to at *Johannesburg* on this the 25<sup>th</sup> day of September 2002 by the deponent who has read, knows and understands the contents of this affidavit, who has no objection to taking the prescribed oath and who considers same to be binding on his conscience.

BEFORE ME,

*[Handwritten Signature]*  
\_\_\_\_\_  
**COMMISSIONER OF OATHS**  
*Willem Steyn*

**SUID-AFRIKAANSE POLISIEDIENS**  
STANDARDBANK KONTAK PUNT  
JOHANNESBURG SENTRAAL  
2002 -09- 2 5  
JOHANNESBURG CENTRAL  
STANDARDBANK CONTACT POINT  
SOUTH AFRICAN POLICE SERVICE

5/09/02 09:22 FAX 787 2541  
 FILE No. 207 05.09.02 12:48 10.

7051903020

REVA  
 PHOC

" R1 123"

**RAMESH SINGH STATES UNDER OATH IN ENGLISH :**

I am an adult male with Id. No. 4206125093053 residing at 69 Bailey Road, Durban North Occupied as a restaurant owner at Club Restaurant, 232 Effingham Rd, Effingham Heights. Tel no. 5637625.

2

In June 2000 I receive a phone call from my attorney Kassim Seedat whom I instructed to collect my rent money. He asked me if I had a Diners Club Card. Kassim told me that he's got a friend by the name of Samuel Bernard who has a friend in London who will make money available to bring into South Africa illegally and asked me if it was okay if Bernard can contact me. I told him that it would not be a problem, not knowing what this all entailed.

3.

The same day I received a phone call from Bernard. He told me that he can only get money to South Africa via a Diners Club Card. I told him that we can meet at Kassim's office for I wanted him to be present when he tells me how the scam works.

4.

The next day we met at Kassim's office at the corners of Cross Street and Prince Edward Street, 1<sup>st</sup> floor C.N.R. house, J.N. Singh and Seedat. The only people present was myself, Kassim and Bernard. I asked them to explain the story to me. Bernard said that he has a friend working in London that can make money available which can be drawn without any trace. I asked them how that was possible. He told me that it would be money that people don't claim for eg. Old accounts that still had money in it. He also told me that the only way he could withdraw the money would be by means of the Diners Club Card. I asked him if there would be any records and if I would be implicated in any way. He assured me that it will all be sorted out in London, for he knows some people in London and that it will never come to South Africa. I asked him what my portion of the deal would be as he made it clear that money would be withdrawn and that I would get some amount from the transaction. He told me that he would give me 100 000 pounds in cash. He would leave on the Thursday, arrive on the Friday and return on the Monday and he asked me to get him from Durban International at 07:30 as part of the arrangements. I was surprised at the amount and asked him how much he would be making, and he told me not to worry about the amount they make but that I would definitely make 100 000 pounds. I asked him who was going to pay Seedat his cut and what amount it would be, and he told me not to worry about Seedat, that he would sort Seedat out.

5.

I was very tempted by the amount and agreed to hand my card over to Bernard. After handing it to him, in front of Kassim, he asked me if I knew my pin number. I told him that I've never used my card in an ATM machine before and therefore do not know the pin number. He told me that I should go to the nearest Standard Bank to get the pin number and that he would come to me at a later stage to collect the number from me. He kept the card with him.

~~\_\_\_\_\_~~

BL

PBB

25/09/02 09:22 FAX 787 2541  
FILE NO. 201 03.03. UC 12.40

TARICABOWES

124

6.

I went to the nearest Standard Bank which was Briardene and I was referred to the Greyville Branch to get my pin number. After I received the pin, I went back to my restaurant where I continued work as usual.

7.

Bernard came to me later the same day and asked me for my pin number. When he arrived there he was accompanied by his son. He told me not to worry about his son being there for his son is okay and that he is the one with the contact in London. I was still under the impression that he would be the one going to London and that I had to pick him up from the airport. I gave him the pin number. He went to the ATM machine down the road and came back a few minutes later. He told me that I still owed money on my Diners Club Card to the amount of R 1218-74. He asked me if I had money to settle this amount immediately for it is necessary to have a clear settlement before he goes to London with the card. He then left and gave me a number to phone him as soon as it is settled. I confirmed that I had the money available. I then went to Briardene branch and settled my account, leaving the Diners Club Card with him.

8.

After I made the deposit I phoned him and told him that the account is settled. He told me to phone Diners Club for it takes up to 24 hours to settle the account on computer and he needed the account to be settled immediately. He also told me not to forget to report my card stolen on Monday morning. I phoned Diners Club and requested them to clear my account, but I was told that it would take up to 24 hour and that there was nothing they could do to settle it immediately. I phoned Bernard and told him what they have told me at Diners Club. He told me that it was alright and that I should not worry about it, but that I must not forget to pick him up from the airport the following Monday, 2000-06-26.

9.

I never heard from Bernard again over the weekend. On the Monday morning I went to the airport at 07:30 to pick Bernard up. I waited for about an hour and a half and there was no sign of him. I decided to go to my Grey street office and phone Kassim for I didn't have any of their numbers on me at the time. I got to my office and phoned Kassim. I asked him if he had heard from Bernard. His reply to this was negative. I asked him he has his number on him and if he could phone him. He told me that he would give Bernard a call right away. About ten minutes later I phoned Kassim again and asked him if he got hold of Bernard. He informed me that the phone was just ringing.

10.

I then went to my restaurant and phoned Diners Club to stop the card. This was at 12:18 dated 2002-06-26 when the call was logged at Diners Club. I never heard from Bernard again.

BL

BB  
AL



TARICABOWES

25/09/02 09:22 FAX 787 2541  
FILE No. 207 US.09.02 12:49 ID:


FAX TUS19US332U

125

11.

A few days later I received an account from Diners Club stating that I owed them R 35138.07. I immediately went to Kassim's office and requested him to get me out of the debt as it was due to him that I landed up in the debt in the first place. I told him to get hold of Bernard to settle the debt. Kassim immediately started legal proceedings against Diners Club disputing the debt. To date I never received any account from Kassim regarding his involvement concerning this matter.

I know and understand the contents of the above statement.  
I have no objection in taking the prescribed oath.  
I consider the prescribed oath to be binding on my conscience.

  
SIGNATURE OF DEPOSITOR

BL BB M

25/09/02 09:22 FAX 787 2541  
F No.207 03.09.02 12:49

TARICABOWES

FAX:70319033020

PAGE 4

126

I know and understand the contents of this statement .  
I have no objections to taking the prescribed oath .  
I consider the prescribed oath binding on my conscience .

DATE : 7/8/2002

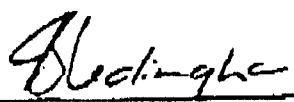
TIME : 1430

PLACE : DURBAN

DEPONENT : 

I certify that the above statement was taken by me and that the deponent has acknowledged that he/she knows and understands the contents of the above statement. This statement was sworn/affirmed to before me and the deponents signature/mark/thumbprint was placed thereon

in my presence, at Durban on 2002-09-07 at 14:35



COMMISSIONER OF OATHS

RANK : Josp.

FORCE NO : 9403041

Benette Leedingham

FULL NAME AND SURNAME  
~~SYNDICATE FRAUD UNIT~~ Commercial Branch  
PROJECT INVESTIGATION TEAM  
23<sup>rd</sup> FLOOR  
JOHN ROSS HOUSE  
DURBAN

SOUTH AFRICAN POLICE SERVICE



25/09/02 09:29 FAX 787 2541

TARICABOWES

1006

~~THIS AGREEMENT~~ made

127  
R

this 26<sup>th</sup> day of July, 1966, among DINERS' CLUB INTERNATIONAL LTD., a corporation organized and existing under and by virtue of the laws of the Dominion of Canada, having an office at 80 Richmond Street West, Toronto 1, Canada (hereinafter sometimes referred to as "International"), THE DINERS' CLUB, INC., a corporation organized and existing under and by virtue of the laws of the State of New York, having an office at 10 Columbus Circle, New York, N.Y. (hereinafter sometimes referred to as "Diners") and THE DINERS' CLUB SOUTH AFRICA (PROPRIETARY) LIMITED whose address is at Cavendish Chambers, Jeppe Street, Johannesburg, South Africa (hereinafter referred to as "Franchisee")

WHEREAS, International has been authorized by The Diners' Club, Inc. to arrange for the licensing of others to operate a credit card business under the name of Diners' Club in Europe, Asia, Africa, Australia, South America and other territories outside the North American continent; and

WHEREAS, International has the ability to furnish various types of assistance and services to persons operating credit card businesses in the territories described above; and

WHEREAS, Franchisee is already operating within the territory referred to below a franchise (hereinafter referred to as "the pre-existing Franchise") granted by International

WHEREAS, Franchisee is desirous of continuing its credit card business in the Republic of South Africa and South West Africa, Botswana, Lesotho and Swaziland

(all of such countries being hereinafter called "the Territory" under the name of Diners' Club and continuing to obtain the services and assistance of International in connection therewith and

T. B. B.