IN THE HIGH COURT OF SOUTH AFRICA

DURBAN AND COAST LOCAL DIVISION

4

DURBAN

CASE NO **3156/00**

DATE 2002/03/04

In the matter between:

DINERS CLUB (SA) (PTY) LIMITED (PLAINTIFF)

and

ANIL SINGH (FIRST DEFENDANT)

VANITHRA SINGH (SECOND DEFENDANT)

BEFORE THE HONOURABLE MR JUSTICE LEVINSOHN

ON BEHALF OF PLAINTIFF: MR P M M LANE SC
WITH MR K J TRISK

ON BEHALF OF DEFENDANTS: MR A K KISSOON SINGH SC
WITH MR M W COLLINS

PROCEEDINGS
ON 7 MARCH 2002
[Pages 296 - 333]

COPYRIGHT:
TRANSCRIBER
SNELLER RECORDINGS

ON RESUMPTION ON 7 MARCH 2002

ALL APPEARANCES AS BEFORE

LEE KENNETH GIBSON (under former oath)

CONTINUATION OF CROSS-EXAMINATION BY MR LANE Mr Gibson, at the adjournment yesterday we were talking about hacking on the Internet, as distinct from the type of encryption system which we have and are dealing with in this case. You will recollect that? --- Yes, I do.

Now, I took instructions during the adjournment, and as I understand the principle involved, where you have the banks in question, is different. Let me explain to you as it was, hopefully, explained to me. That the hacker will go on to the web through his ISP, his Internet service provider, and that the protection system for the bank lies in a firewall. Would you agree with that? --- Correct.

Now that firewall is what is first attacked. If they can breach the firewall they then get through to the various servers. Is that correct? --- Correct.

Those servers reside in what is referred to as a demilitarised zone, a DMZ. --- Correct.

LEVINSOHN J Just explain the DMZ to me.

MR LANE Yes, M'Lord, it is only secured - it is a pack of servers which then has data attached to those servers. The servers have some form of protection but it is not the same form protection that you have when it comes to dealing with encryption. So the main protection unit lies in the firewall which then has an area behind the firewall which is less secure, if I can put it that way.

LEVINSOHN J Do you agree with all that, Mr Gibson? --- Yes, correct.

So servers are the banks' computers which store the information?

MR LANE That is so, M'Lord, and respond to the client coming in and making a request for bank balances, etcetera. Now, those servers have some protection on them but not a very sophisticated form of protection at this point in time. Would you agree with that? --- Correct.

And they sometimes have data attached to them? --- That is correct.

And that data often contains, for client/bank relationship, the PIN or access code number of the client in clear form? --- That I wouldn't know. I don't know how the banks would store that information.

You see, the difference, Mr Gibson, is that this had got nothing to do with encryptology, this form of protection. Would you agree with that? None of this has got to do the encryption of information. The attack is entirely different. --- Can I just take a moment to think about that?

Yes, certainly. --- Just clarify how the attack is completely different.

Well, none of the information contained in this, either the firewall or in the server or in the data is in encrypted form. --- Correct, ja.

Now, turning then to the example you gave where the DES or

the SDES, that's the encryption standard was that, I believe what you were referring to was a challenge issued by a company known as RSA, Rivest Shamir Alderman. --- Correct.

Is that correct? --- Correct.

They were, in fact, the designers of the DES system. Is that correct? --- Well, initially, ja. I think the DES was originally designed as a part of IBM, but, yes, they are certainly expert in the field of encryption codes and encryption algorithms.

And they issued a challenge to the market to devise a system that could break the single decryption - data encryption system. --- That's correct.

For an amount not more than US $250 000. --- Well, they seem to have an on-going competition which is every January and every July. They issue a challenge and it's based on the number of bits in the key. They start with a 40 bit key and work upwards and, depending on how far you get up the scale, that's the amount they will pay out if you break it.

I'm sorry, perhaps I didn't phrase my question properly. One of the criteria for entry into the competition was that those who entered could not spend more than $250 000 on manufacturing the equipment necessary to break the system. --- That might have fallen away because when I see some of the - no, look, okay, I would agree with that, $250 000 because with the way that the power of computers increases, you know, Moore's Law says that you double your power every 18 months. What it means is that every 18 months for your $250 000 you're doubling the power that you can get to try and break

the code.

LEVINSOHN J When you talk about a bit, is that a measurement of memory? --- Yes, M'Lord, that is - when you get inside the computer, when you get right down to the basics, that is how the information is stored because computers can only understand either something is switched on or something is switched off and using that, if it's switched on, they designate that as being a 1, which is a 1 bit. If it's switched off, they designate that as a 0 which would then be a zero bit.

That's the basic principle of computing, isn't it? --- That's your basic principle of computing, ja, using binary code.

So the 1 and the 0? --- That's correct, yes, M'Lord.

MR LANE But what is clear from all those exercises, is it not, Mr Gibson, that the machines that were utilised to attack the encryption systems were specifically designed and built computers? --- Correct. They use different methods. It was not only specifically designed. What some of them did was to harness many, many computers on the Internet and use a combined force of computers to attack the codes, and those were also successful. This is different techniques.

But quite apart, an attack would have to be adopted under those circumstances, a very particular and large frontal attack. --- Very much so. It's what they call a brute force attack and, yes, you certainly have to have power in your machines.

Other than these challenges, I am instructed that there has never been an instance, and this is in the knowledge of Standard Bank

or indeed we have spoken internationally as well, where the encryption - that is the encrypted PIN and the information appearing on the mag stripe has been decoded whilst in encrypted form or being transmitted in encrypted form. Do you know of any incident? --- I have no knowledge of that.

LEVINSOHN J Just repeat that question again. I've got to write it down. Never been an occasion?

MR LANE Where information in encrypted form, either being stored in encrypted form or being transmitted in encrypted form, i.e. consisting of the PIN and the mag strip information, has been deciphered, if I can put it that way.

LEVINSOHN J What's your comment on that, Mr Gibson? --- My comment was that I don't know of any either. However, with what I have read and my experience that only one-third of any instance actually gets published, I don't know whether it could be in the two-thirds that don't get published.

On the facts of this case, if there was any attack on the encryption of the PIN number and the mag strip, it would have had to happen in South Africa? It couldn't have happened elsewhere or don't you agree? --- No, I agree - well, it depends once again, because remember that PIN is stored immediately the card is produced. That PIN is stored in London so if there - I mean if anyone could get access there it could have happened in London. I'm not saying that it did but it could have because the PIN was stored elsewhere.

MR LANE Let's just look at that proposition, Mr Gibson, and let's again keep in mind this concept of probability. You did speak about

the procedures regarding the tapes. Now, you will recollect from your reading of the expert summaries filed by the plaintiff that when a card is issued a PIN is immediately generated. So every time a card is issued a PIN is generated, whether it is issued or not. --- Correct.

That is done and recorded by the Standard Bank mainframe on a tape which is then sent to the United Kingdom. --- That is correct.

LEVINSOHN J Just repeat that, please.

MR LANE Yes, M'Lord. The PIN which is generated is then - is on a tape which is then sent to the United Kingdom, who then on-sends that tape to Germany, where it is then stored in encrypted form in a black box there.

LEVINSOHN J Are we talking of Diners cards now?

MR LANE Yes, this is specific to Diners Club, M'Lord. The storage in Germany is in TDES, triple data encryption standard, which I'm told not even these challenges have broken TDES. --- That's correct.

Do you know of any instance? Because certainly we are told that TDES at this point in time is completely inviolate. Nobody has ever broken TDES. --- In my knowledge, it certainly has not been.

So if it is stored there, that rules out any attack whereby the PIN could have been got in Germany. Do you agree? --- An outside attack, yes. I don't know the procedures of access internal to the system.

LEVINSOHN J So there might be a sort of - let's call him or her a Trojan horse within the system? --- Correct, M'Lord.

That could undermine the system. But from outside it's most unlikely that it happened? --- That's correct, M'Lord.

MR LANE Now that happened in - in this case happened in 1997. In other words, that tape containing Mr Singh's PIN was transmitted in February 1997. So are you really suggesting that someone, to access that PIN from that tape, waited three years before he made then his attack on the 4th and 5th March? So you think that's probable? --- I can't say whether that's probable or not, M'Lord.

I'm instructed that the black box is a Racal - you know a Racal? It's the black box that sits in Germany. --- All I know ...[intervention]

LEVINSOHN J The black box is what?

MR LANE A Racal, R.a.c.a.l, M'Lord. --- I know of it. I have no experience of actually working with it.

And I am instructed that the Racal does not release the PIN in clear form at all, and therefore there can be no Trojan horse in the system. --- Well, that would solve that problem then.

The PIN is not stored in South Africa. Do you recollect reading that? --- I believe that is correct, yes.

And you will recollect the reason for that is because of the creation of what is referred to as PM key a PIN master key. --- Right.

Do you accept that? --- Yes, I accept that.

LEVINSOHN J Just explain to me what the PIN master key is.

MR LANE The PIN master key, M'Lord, is a key which is set up which is able to verify when the PIN comes in in encrypted form - by a process of encryption and decryption, is able to verify the PIN and is also able to issue the PIN. It's a process of the encryption system, M'Lord. In simple terms, M'Lord, if I can explain, the systems are set

up in such a way that keys are created within the systems. Zones are created between the systems which are then able to communicate one to the other and by that creation I've got they use is a series of keys, algorithms, which then through a mathematical process encrypt the PINs and the information and verifying both[?] issue of the PINs themselves. That is how the security is maintained and ensured. Perhaps just for the sake of completeness, Mr Gibson, Mr Bonfra - you remember Mr Bonfra is one of the experts being called by the plaintiff? --- I heard the name, yes.

He deals - he gives an opinion. It's his second opinion, which is paragraph 111 of his expert summary, and he says in his opinion initial generation of the PIN is safe and secure and he gives his reason,

> "The process of PIN takes place with a highly secure object code. The source code to the object code is not available to Standard Bank South Africa. As a result of this, Standard Bank South Africa cannot apply any changes, illegal or legal, to the object code. Access to and use of this object code is protected by Top Secret, which is a software package, a computer access and authorization control system."

I assume you actually wouldn't know about those systems. --- No, I mean I ...[intervention]

But you wouldn't dispute that? --- No, not at all. I have agreed that the systems - that particular aspect of the system seems

very secure. I mean, I will agree to that.

Yes. Now we spoke previously about the black box and you also made reference to the black box in your evidence-in-chief. Now a black box is what is sometimes referred to as an HSM, high security module. Is that correct? --- According to the documentation, that's what they call it.

Sorry, a hardware security model. Now, do you know anything about the operation of the black box? --- No, no. That's why it's called a black box, sir.

So again you wouldn't dispute the testimony that it's tamper-secure? --- No, I wouldn't dispute that.

LEVINSOHN J Is this the black box that's kept in Germany?

MR LANE That is so, M'Lord. In fact there - yes, this is the black box kept in Germany, M'Lord. The PMK is also in a black box. That's in the SBSA in the mainframe on the Standard Bank computer. And there's also one at DCIC in the UK. Every system which, in fact, deals[?] and houses those important keys such as the PM key or whatever, M'Lord, they house them in a black box. Now you spoke in your evidence about the trapping of information. Remember that? --- Yes.

Trapping of information. Now, trapping information, as I understand your evidence, is that last portion that you refer to as the most dangerous portion. --- Correct.

It is between the computer and the printer, that last portion when it's in the clear. --- Ja, that's one of the dangerous areas. There is another one but we'll - we can come to that.

Well, let's deal with that one first because I don't remember you mentioning any other one. Now, there - that is between the computer and the printer there is approximately a metre long cable which it has to travel along. Would you agree with that? --- It could be a metre, could be three metres but ...[intervention]

A short distance. --- A short distance. It's not a kilometre.

LEVINSOHN J So this is between the computer and the printer. There's a short ...[intervention]

MR LANE It's a very short length of cable. So it would be visible. It's a visible cable. Anybody looking at that machine and the printer could see that cable? --- Correct.

Now, I'm instructed in relation to this particular cable which is now from the CTOS, do you know what a CTOS is? That's computer technology operating system. --- Right, okay.

Which is the package given to Windows, the operating system which receives this information in the PIN generation. That because it is the CTO system they cannot use a standard parallel cable. --- Okay.

Now, does that make it more difficult to tap into? --- What kind of cable are they using?

Well, it's a specially-made customised cable dedicated to the CTOS operation. --- Does it also operate in parallel mode or does it ...[intervention]

No, it doesn't operate ...[intervention] --- Or does it operate in serial mode?

I believe so. But it is custom-made cable. Doesn't that make

it much more difficult to simply just tap into? --- Tapping into the cable, yes, but that's not where I would try and tap in if I were trying to break the system.

Where would you tap in? --- I would get into the machine itself that is doing this print, because that's what I said yesterday. I said some time or other in that computer that does the print your PIN must be in clear form or plain text and somewhere or other, if you have the knowledge, you can trap it in that computer.

LEVINSOHN J And where is that likely to occur? In the printer itself? --- It would probably be - it depends on - not so much in the printer itself but in the computer that does the print because, as I recall, they spoke about a spooler. Is that right?

MR LANE Yes. --- I mean that - the printer spooler is the one now that's doing the print. Now somewhere or other that is stored for print, be it in the memory of the computer, be it a hard disk, wherever it is, somewhere that is in plain text and can be got at.

Let me just correct something CTOS is convergent technology operation system. First of all, do you know of any incident where that has ever happened? Where someone has actually installed something in a spooler which has recorded all the PINs? --- Certainly not, sir, but what I'm saying is that is - if I were attacking a machine, that's where I would attack it.

Well, let's try and look at the historic situation and look at the probabilities. You've never heard of one. The plaintiff has never heard of one. Standard Bank has never heard of one. So someone hasn't yet manufactured and installed such a module, have they? ---

Or someone hasn't reported it, sir.

Well, you keep coming back to that but surely it's in the interests of the industry and the industry would know - Standard Bank would know. Standard Bank is involved in the process, isn't it, Mr Gibson? --- Yes, they are.

Surely you are not suggesting that they would not even tell me in this case that that had happened? --- That I don't know, sir. I really do not know.

You really wouldn't make that suggestion, would you? You've got no grounds for making that suggestion? --- No, I have no grounds for making that.

LEVINSOHN J All you are really saying is that it just may be possible but, in reality, there is no fact to support that? --- To support that. Absolutely not, M'Lord.

MR LANE You see, the other factor on that is that the CTO system, because it is a dying[?] platform there are very few people who actually know about that technology at all at the moment. Do you know anything about that? --- Not at all, sir, but as I said yesterday, in security you never base on assumption - your security on the assumption that people don't know things.

Now you spoke in your evidence at some length about the four digit, the numeric PIN. Have you read what Mr Bonfra says about that? He deals with that at paragraph 113, page 43 of his summary? --- I don't recall the exact wording, sir.

LEVINSOHN J Which PIN is that?

MR LANE This is the four digit PIN, M'Lord, the permutations on the

four digit PIN and the security value on that. This is his opinion. M'Lord, it's a couple of pages long. I wonder if I should put this in front of the witness and - or let me read it out. He says this,

> "Notwithstanding that a four digit PIN results in there being a finite number of permutations, that is 10 000, and that, as a consequence, there will be cardholders of the plaintiff who can have the same PIN number, this does not compromise or otherwise detract from the integrity of the card system implemented and employed by the plaintiff."

His reasons,

> "The PIN number issued by Standard Bank South Africa on behalf of the plaintiff, as referred to in paragraph 60 above, is a derived PIN, as opposed to a random PIN. A derived PIN arises in circumstances where the account number allocated to a cardholder of the plaintiff would detect the permutation of the PIN and ensure that the same PIN number is generated every time the PMK ..."

That's the - well, you know what it is. --- Mm.

> "... generates a PIN in respect of the specific account number."

M'Lord, perhaps I could ...[intervention]

LEVINSOHN J I just want to ...[intervention]

MR LANE Sorry, M'Lord, I think it's the furthermost bundle, just looking at the size of it. It should be ...[intervention]

LEVINSOHN J This is the notice in terms of rule 36(9)(a).

MR LANE Have you got a spare copy?

LEVINSOHN J This is the first expert statement?

MR LANE The first expert statement, M'Lord. Page 43 - starting at page 43, paragraph 113. M'Lord, I've read paragraph 113.1.

LEVINSOHN J Yes, I've got it.

MR LANE And I was into 113.2 at the top of the page at 44. Perhaps you'd like to just glance through that and catch up to where I was, Mr Gibson. Yes, now, it carries on,

> "The reason for this is that all PINs generated by SBSA ..."

Which is the acronym for Standard Bank of South Africa,

> "... on behalf of Diners Club are so-called system-generated PINs. The cardholders of the plaintiff not being able, given the manner in which the system is operated, to select their own PIN numbers or change the PIN number allocated to them by the system. System-generated PINs are created using an encryption key, a standard algorithm, the card number and decimalisation table used to transform the PIN number to numeric form

> from hexadecimal form. The encryption key used is the MPK. The first four digits of the generated number are then used as the PIN. Due to the static values that are input into this process the PIN will always be the same for a particular card number. The marriage between the PIN and the card number will be always be unique to the specific card number. Given that PIN block format ISO zero is used in the PIN verification process there will on this basis be no scope or possibility of two cardholders of the plaintiff having the same PIN number, having their transactions confused one with the other. The marriage will ensure that transactions pertaining to a specific card number ...[indistinct]... the PIN associated therewith might be the same as another PIN issued on behalf of the plaintiff are correctly debited and allocated as against the account which correctly and legitimately falls to be debited."

Do you agree with that? --- Yes, I agree with that. That's pretty much standard practice in the industry.

Perhaps while we have the expert summaries I could deal with them. You will appreciate that, from having read the summaries file

on behalf of the plaintiff, that the approach adopted is case specific. In other words, the witnesses, if they are experts in, for example, the procedure, the Standard Bank, talk specifically not just about industry norm, but also the specific to the mainframe computers, whatever it is that has been utilised in the system be it at Standard Bank or at Diners Club. --- Okay. I understand that.

Yes. And that a lot of the opinions are not only based upon the system, the norm in the industry, but also to the facts of the matter. They have addressed the facts. They have been advised as to a series of facts and their conclusions are driven not only by their particular knowledge of the equipment in question in the industry standards and norms but also the facts of this case ...[indistinct]... from your evidence. --- I understand that.

Yes. Now, it's incumbent upon me to put the various versions of these experts to you but you've had an opportunity of reading through all their statements so I'm going to try and do it by way of exception rather than trying to read what amounts to hundreds of pages of evidence to you. Is that acceptable? --- That's acceptable, yes.

Let's start with Mr Bonfra. Is there anything in his statement which you particularly disagree with? --- Sorry, can you just ...[intervention]

Mr Bonfra is the first one on the file - Petrus Adrianus Bonfra[?]. --- I'll just get to that. Okay. There was nothing of exception there that I recall.

If you then go to the next document. That is the testimony of

Donald Jardine. Donald Jardine is the programmer of Microsoft Auto-e division of Standard Bank. It should be the next document in the file. --- Yes, I have it.

Can you look at it in the same context? --- The only comments that I had on that one was that the issue of a PIN is certainly the danger area because the PIN is in plain text and if any problem can occur that is one of the places where it would occur.

That's the possibility we've just debated? --- Yes.

Yes. But otherwise you accept what he's got to say? --- That's right, ja, I mean he's ...[incomplete]

If we can go to the next summary then, which is the testimony of Michelle Ericson. She is the network security and encryption service manager of Standard Bank. --- Ja, I don't have any problem with that one.

LEVINSOHN J It's a lady, isn't it?

MR LANE That is so, M'Lord. You have no problem with that? --- No.

No problem with that. Let me go then to the testimony of Michael Pinnit[?]. That's the next one. Mr Pinnit talks about the establishment of the zone master key. --- No problem with this.

You accept his testimony as well? --- Ja.

The next item, which is No 5, is Michael John Davidson. He is the person responsible for developing mainframe application software and ensure that it meets Standard Bank's requirements in terms of functionality, performance and integrity. --- Sorry, there was just something I was looking for here. Can I just query point 4.4? This is

with Michael John Davidson. I just want to know what happens to that tape when they say the tape gets recycled. "The plaintiff thereafter returns the tape to it and it recycles the tape." I just need to know the - whatever information is on there, how it is cleared from the tape.

Perhaps the easiest way of dealing with that, Mr Gibson, is this, because I think you've already agreed on the probabilities that the likelihood of something happening in 1997 and then suddenly surfacing in relation to one PIN three years later is highly improbable and that really the tapes don't play any integral part in this matter. You have agreed with me on that probability, haven't you? --- Ja, about that one particular PIN surfacing.

Well, then this is the case that we're dealing with here so in so far as that's concerned I don't think you need to worry. I understand because you said that you're concerned that it's not overwritten or erased ...[intervention] --- Or how the overwriting takes place.

Indeed, but it's the probability that we are talking about here. Three years ago one PIN, three years later, the likelihood of that happening, the probabilities, you concede that it's not going to happen so I don't think we need to be sidelined by that. --- Okay.

Otherwise you accept his testimony, do you? --- Yes, yes.

The next affidavit is Mr Pretorius. I don't know whether - perhaps you can assist us in looking at Mr Pretorius, as he talks about the systems in the bank whereby issue of PINs are logged. Your Lordship will recollect you asked, M'Lord, as to whether we had checked as to the number of times the PINs were issued in this

matter. This is the expert testimony that deals with the computer system which logs every time a PIN is requested or issued. Do you have any quarrel with that? --- I can't help you on that one at all.

After that you will see a computer affidavit by Mr Pretorius and I'd just like you to look at the back of that because, being - a document attached to it - being acquainted with computers you would recognise that as being a computer printout, wouldn't you? --- Correct, yes.

LEVINSOHN J Where is this now?

MR LANE M'Lord, it is the next document, No 7. That's where he derives the information for his expert testimony. Now, we go to then document 8. That is the testimony of Kevin de Vaughan[?]. Do you have that? That's document 8. --- 8, Kevin de Vaughan, yes.

He is the assistant manager, group fraud and security of Lloyds TSB Bank, and he talks about very much what we were talking about yesterday, the ATM activity reports, that he's examined them, there was a balancing of the machines, etcetera, and he attaches to his expert summary - it's at C3, I think. It's got C3 at the top of it. I'm sure you've seen documents similar to that, Mr Gibson. --- Ja. Also a computer printout.

Also a computer printout. Yes, this is the computer printout of the operation of those ATMs in question over the 4th and 5th March 2000. Do you have any quarrel with what he says? --- No. There was no quarrel with this. As I said, my query was just why they weren't picked up as being abnormal.

Right, let's go to the next one. That's Mr Cummins. That's

document 9. He is the senior manager with National Westminster Bank DRC, Natwest. His evidence is very similar to that given by Mr de Vaughan, and he too - just have a look at the document. You will see his document at N2 attached. Do you recognise that document, that type of document? --- It's the same.

Is that the same - it's a computer printout, is it? --- Mm. Ja, just listing all the transactions that have taken place.

Yes. Of course, if you have a look at that - perhaps we could just briefly look there - another way of ascertaining whether a machine is operating correctly is to see whether it is defaulting anywhere else in other transactions. Wouldn't that be correct? In other words, if I've got a continuous record of a machine operating ...[intervention] --- Yes, yes.

... if I found that there were malfeant[?] transactions either side or elsewhere, that would be a way of telling me that the machine was not operating correctly? --- Yes, yes.

Well, these records establish that that wasn't the case because if you look through them you will see that there is a malfeant down record or misfunction record on these machines. --- Just a query on all these. Are all these ATMs very fast? I mean do they issue cash on a very, very quick basis?

That I couldn't answer. That is something which would have to be answered in the fullness of time but what we can tell you is that the machines balanced. --- Ja, okay. No, it's just that they issue cash at sort of, at a transaction a minute and it's just a question I have as to whether they are ...[intervention]

Yes. --- ... new machines or do they work very quickly.

I can show you the machines, in fact, if you'd like to see them. There's a bundle here. We have a picture of all the machines in question. M'Lord, it's in the little bundle, Exhibit B. If you want to ...[intervention] --- No, I just asked the question because I ...[intervention]

Well, what one does know, in fact, industry norms are getting faster and faster in those ...[intervention] --- Sure.

Is that electronic information can be transferred in a matter of 15 to 17 seconds and sometimes even faster. --- Right.

The whole verification pattern can take, in its full cycle, travelling even from London through Germany back to London, can take as little time as 15 to 17 seconds. --- Sure, ja, I agree. So, I mean, it's quite possible to distribute a transaction a minute. It's quite possible.

Certainly, quite possible, yes. --- Okay.

Let's have a look at the next one. That's Mr John Paul Clow[?]. He is the senior investigator, security ...[indistinct]... with Abbey National Bank in London. --- Sorry, I seem to have lost - what number is this?

That is No 10. --- Sorry, I jumped one ahead.

He gives the same type of evidence. He attaches what is referred to, I think - if you have a look at A2, you will see - perhaps you would just identify that for me. --- Yes, once again a list of transactions.

Is it a computer printout? --- It's a computer printout, list of

transactions, listing for each terminal.

And what Abbey National have is a special piece of software which, in fact, records any problems with the ATMs and if you look at A9 you will see what's referred as the Gasper workstation. I don't know if you've heard of a Gasper workstation. --- No, certainly not.

Well, that's one of the checks on their particular machines to make certain that they're operating correctly, and again would you agree this is a computer printout? --- Yes, yes, what looks like a copy of a computer screen. That's what it looks like to me.

Yes. Any problems with Mr Clow's evidence? --- No.

Go to the next one then, that's Mr Derek Wilde. He is the manager at card fraud services of HSBC Bank in London, and attached to his expert summary is, as H2, you will see the audit log. Have you seen an audit log before? --- Sorry, which one is that? Is that H ...[intervention]

That's Mr Derek Wilde and it's H2. --- Yes, okay, H2.

That is what he refers to as the audit log for those transactions. --- Same thing, list of transactions coming out.

Yes, for those, and again a computer printout? --- It looks like a tally roll of sorts.

You wouldn't recognise that as being a specific computer printout though. --- Well, a very narrow computer printout.

Yes. Right, any challenge to Mr Wilde? --- No.

Then we have the testimony of Alexander Lekenby[?]. Mr Lekenby is the security administrator and senior customer support analyst for Link. Now, you remember on that diagram, Link is the first

switch organization which sits between the host bank and TSN, the second switch organization. --- I see, and this is similar to Saswitch.

Yes, exactly. What it does, it receives the information from the host. It recognises where that information goes. If it is directed to one of its members it switches it directly to its member. If it has to go to another switch, in this case TNS, it switches that to TNS but it then keeps a record and perhaps I should at the same time refer you to the document under 13, which is the affidavit of Mr Lekenby which attaches the computer print-outs which were generated by Link in relation to these and other transactions and they are annexed as Link 1 and following. Do you recognise those? Are those computer printouts? --- Ja, difficult. Well, they're just printed on pages.

They have been printed on paper, yes. In other words, they've been photocopied. --- Ja, I'm just trying to see if I recognise anything in there. Okay. It looks like terminal numbers and ATM numbers and ...[intervention]

Well, absolutely - you're absolutely right. What they do is, it records but it gives a code to everything so there is an absolute record from the terminal it came from, the bank it came from, the customer it's going to be switched to. It's in this line with all these codes and I'm afraid don't ask me to unravel it now because it's quite a complicated process but the net effect of it is that from that you can unravel exactly the source and the destination of that piece of information. --- Okay.

Do you have any challenge to Mr Lekenby? --- No, no.

Right, the next one you will get there is Louise Markham. It's

an authenticating affidavit by Louise Markham. That's document 14 in this bundle. Louise Markham signs, she's employed by Transaction Network Services, TNS is the acronym, which is the second switch organization, and she's the business process and compliance manager. She attaches documents to her affidavit. You will see those from TNS1 onwards. First of all, do you recognise those as computer printouts? --- Yes, I do.

And again this is a little easier to identify because it's in a less ciphered form because you actually trace the time, the trace number, the card number, the type of transaction, the amount acquired, the failed transactions, the response codes, etcetera, going through the TNS switch organization. So again on the audit trail of these transactions we can trace it through these. Do you accept it? --- I accept it, ja.

Then the affidavit - sorry, expert notice of Adrian Walker. Mr Walker, you will see he is there and he is in charge of the CAFE system. --- The card authorization front ...[inaudible] ...[intervention]

Yes. --- ... system.

You've seen that often enough. --- Is this where the authorization for the transactions takes place?

No, no. The authorization doesn't take place there. It's again a process by which the information is transferred. --- Okay, all right, sorry.

Bearing in mind that I explained to you that the black box which contains the encrypted PIN is situated in Germany. --- Right, okay. No, sorry, I was just asking, you know, if I'm going to draw cash,

where in the system does the authorization come from?

The authorization goes through the Diners Club circuit. You've seen - would you like to look at that diagram because you can, in fact, see it ...[intervention] --- Ja, I've got a picture of it, ja.

But bear in mind - let's not again get sidetracked like we did yesterday, that anything downstream of the ATM for the purposes of this case is irrelevant because what you've got, and you've agreed to it, you have to present at the ATM the card with the PAN and the PIN which coincides. So if there's a breach in the system it's got to happen before that. [Indistinct]... that information is travelling down the network which travels from ATM to Germany and back again. --- Okay, no, I was just wondering where the authorization for each cash withdrawal takes place.

I don't think you need worry yourself but it doesn't happen here. --- Okay.

But you've read this because he talks about CAFES and CHAMS[?]. No challenge to that? --- No.

Now let's go to Alan Mortlock. He is the next document. That is again the expert testimony of Alan Mortlock. He is the business interfacer between the technical groups CHAMS and CAFES and certain franchisees and he is based in Farnborough. [Indistinct]... opinions. His opinions start at paragraph 19. --- Ja, I did have one question with this. I couldn't make out from this whether - is this using the secure electronic transfers - SET system? I couldn't make out from this as to whether at this stage this is using SET or not.

Have a look at his opinions. His opinions start from

paragraph 19, and see if you have any difficulty with those opinions. --- There was a word that I wasn't quite sure of. They said "The data management processes in place in CHAMS are fully-tested programmiture". Ja, I remember this and that was just a question mark that I have on that.

Let me ask you this. Isn't SET only applicable to the Internet, not applicable to this system? I am instructed it only applies to the Internet. Is that correct? --- Well, ja, I would think it is. So there's no Internet transactions here?

No, none at all. --- All right. If I buy something over the Internet ...[intervention]

This has got nothing - you must take my assurance, there is absolutely nothing here which is on the Internet. --- Okay, so it's completely different checking systems for Diners Club if I use something over the Internet.

Totally. This has got nothing to do with Internet. --- Okay.

Do you accept that? You don't know different? --- I don't know any different.

Any challenge to Mr Mortlock? --- No.

Mr Byrd is the next one. He is the development manager for certain applications for Diners Club, United Kingdom. Any challenge to Mr Byrd? --- No.

Next you have the affidavit of Mr Prospero. Perhaps you could look just at the annexure to that. Would you recognise that as being a computer-generated statement? --- Yes.

Right, and then if you would have a look at his next affidavit.

This is what they refer to as the recap statements and they are all attached here. This is the information which flows through to South Africa encapsulating the transactions in question. --- Sorry, I can I just ask a question here? He is in South Africa. Is that right?

Yes. --- He's with Diners Club in South Africa?

Correct. --- Okay.

And the affidavit is also by the same deponent, Vitor Manuel Seixas Prospero. Again it's just a confirming affidavit. I just want you to look at the annexures. --- I've got the first one. Can I just ask, just to clarify, I didn't understand the difference between transaction date and the date received.

Yes, well, don't worry about that, Mr Gibson. This is information which they capture on the computer. It's something which we will explain ultimately but I just need you to confirm that that is a computer-generated statement. --- Okay, all right. No, I'm just raising the queries that came up in my mind.

I understand. I understand. I don't think you need to worry about that. Then his next affidavit, as I say, attaches the recapitulations. Would you again just look at the annexures. Don't worry about the content of the affidavit. Will you confirm that those are in your experience computer printouts? --- Yes.

And if you then look at the final document, which is an authenticating affidavit by Andrew Brett in the United Kingdom. He is with Diners Club International. --- Am I missing that one.

Right at the end of your file. Perhaps it's not. I am instructed it's not. I will hand you a copy of that. --- Thank you.

Might I ask whether this is, in fact, in Your Lordship's file.

LEVINSOHN J No, it's not. This is Mr Brett's?

MR LANE That is Mr Brett. Because I think it came after these bundles were prepared, from England. M'Lord, might I hand up a copy of Mr Brett's authenticating affidavit? We have given a copy to our learned friends. Again it's simply - and what I wish the witness to do is to look at the annexures to it and confirm that these constitute computer printouts. --- Correct, those are computer printouts.

And again this all ties back to the evidence of being able to audit the transfer of information from the ATM through the various switch organizations to Diners Club, UK, via that circle, and back to South Africa. You've looked at that in that context? --- Yes.

Yes. Now, I only have one area that I believe I must still canvass with you and that is you spoke about a sniffer on the ATM. Do you remember that? --- Yes.

And here again we use the concept of sniffer in its relatively loose ...[intervention] --- Generic term.

Generic term. Now, it is correct that the pad is coupled to a cryptochip? At an ATM. --- Yes.

Coupled to a cryptochip. --- Yes, the encryption takes place in the keyboard itself or in the key pad itself.

Would you know what kind of cryptochip is used typically? --- No.

I am instructed that it's a Dadas[?] 5002 FP processor. Have you heard of that? --- I can't say I have, sir.

And that controls the pin pad. So as you put that information in it's encrypted immediately. You have to do more than nod your head, I'm afraid. --- Yes. Sorry.

So I am instructed by installing a sniffer in the ATM key pad it simply is not going to operate. It will simply not be able to get a PIN in the clear by actually putting a sniffer there. --- The ones that I have - I have discussed this with some of my colleagues at the university, these devices. There is one that actually detects the physical pushing of the key pad because they understand - right, they understand that the cryptology happens right there, and maybe that's not considered a sniffer. I don't know.

But do you know of those being put into operation anywhere in the world? --- Well, I mean, you certainly are hearing reports that this is one of the ways in which they are getting stuff out.

Do you know of any instances in South Africa? --- No, not *per se*.

Standard Bank and Diners Club have no experience of that in South Africa at all. Now, that would be a relatively sophisticated piece of equipment, wouldn't it? --- Yes, it is, yes.

Quite difficult to manufacture and quite costly? You need a fairly sound scientific background? --- Well, it sounds like a $1 000 dollar touch I would imagine.

LEVINSOHN J Just explain to me, what is the hypothesis here? The hypothesis is that as the customer is busy tapping in the actual digits of the key, there will be some sort of machine able to intercept it ...[intervention]

MR LANE To detect it, physically detect.

LEVINSOHN J Physically what numbers have been tapped in? --- Correct, M'Lord.

Apart from the question of those numbers being translated into code on the machine, this is a way of just intercepting it, diverting it, so to speak? --- Correct, M'Lord.

MR LANE Now, to do that though, you'd have to physically alter the machine, wouldn't you? Because you'd have to actually fit something into the machine. You'd actually have to physically tamper with the machine? --- Ja, look, the understanding that I have of this is that they would normally do it in a fairly remote ATM. In other words, I mean a physically remote ATM, or in places like New York, where they have a lot of ATMs in stores, which is away from the banks. That's what I was talking about in particular there.

But it would require a physical appendage to the machine? --- Yes, yes.

And it wouldn't be just one incident. This would be put on to collect a whole series of PINs? --- Yes, that's right.

LEVINSOHN J So the hypothesis then is that in this particular case, on the facts of this case - I don't know how many machines are involved but in each one of those machines there would be this device installed? --- No, no, M'Lord, it's to pick up the PIN number. Initially to steal the PIN number is what they use it for.

But it would be physically located on those machines? --- That they are using for stealing the PIN numbers, yes.

MR LANE Well, let's take the - we have a relatively unique situation

here because we had the PIN issued on the 16th February. It's common cause that the PIN is not utilised at all, whether it be point of sale or ATM, between the 6th February and the 3rd March. So therefore no opportunity between those two dates of obtaining card and PIN or either. 3rd March it's utilised, two transactions, two failed transactions, two Nedcor machines. No - you've accepted what Mr Pretorius says in terms of the operation of those machines and there is no malfeant report, misfunction report on those machines. So there was no attack on those machines. Or let's assume that there was for a moment - some form of device installed on those machines, as unlikely as it would seem. How would they then have got the card? Because they also needed the magnetic stripe information and the sniffer doesn't or the mechanism doesn't help you get the card, the magnetic stripe information, does it? --- No, you don't get the magnetic card information but once again, from my understanding of how - and I must say I have not seen these things in operation, but there are normally two devices put on to the ATM. The one would be that you have to go through it to get your card into the machine and the other would pick up the PIN. But, as I said, they normally have to do it on remote ATMs because of - as you say, it is a physical device that you have to put on to the machine.

Well, again, we have some difficulty with that proposition because we haven't (a) heard of this mechanism at all, Standard Bank or Diners Club, and (b) given the passage which the card takes into the machine and out, the probabilities of being able to manufacture something which in that space could act as a sort of false mechanism

seems to be rather remote. You've never seen one of those machines? --- I've never seen one, definitely not.

So this you've just heard about? --- That's right, in discussions with my colleagues at university, just discussing these devices that are now being used.

LEVINSOHN J Mr Lane, is your evidence that these two machines, the one in Stanger and the one at the airport have been inspected and there's been no malfunction?

MR LANE That is so, M'Lord.

LEVINSOHN J Nothing has been cannibalised on to that machine or engrafted on to it?

MR LANE That is so, M'Lord. That is my evidence and that is what Mr Pretorius - we produced that evidence. So we can, on the facts, M'Lord, exclude that entirely. We have spoken to Nedbank and Mr Pretorius has investigated the situation, so there's no evidence whatsoever, M'Lord. No further questions, M'Lord.

NO FURTHER QUESTIONS BY MR LANE

LEVINSOHN J Do you want to take the adjournment or will you be short in re-examination, Mr Kissoon Singh?

MR KISSOON SINGH I have no re-examination, M'Lord.

NO RE-EXAMINATION BY MR KISSOON SINGH

LEVINSOHN J Thank you, Mr Gibson. That will be all.

LEVINSOHN J We will take the short adjournment.

COURT ADJOURNED

ON RESUMPTION

MR KISSOON SINGH M'Lord, at this particular point in time I'm instructed to ask for an adjournment of the trial. There are a number of reasons why the adjournment is being sought, the most significant of which, M'Lord, is that the defendants are in the situation where they require expert assistance from persons involved in more specific areas of the computing industry, particularly in the field of encryption and decryption and in systems analysis, M'Lord.

LEVINSOHN J Yes. Wasn't that manifest to the defendants when they read the summaries, that they might have this problem?

MR KISSOON SINGH M'Lord, the summaries were delivered shortly -in fact, M'Lord, if I'm not mistaken, at the time of the rule 37 conference, which was on the 7th February. We have made several endeavours to locate witnesses. I have an affidavit from my instructing attorney. I made a copy available to my learned friend ...[intervention]

LEVINSOHN J Well, before we get into all that, Mr Lane, what is your attitude to an adjournment? The case would inevitably have to be adjourned. We are looking at a day, or losing a day, aren't we?

MR LANE We're losing a day, M'Lord. The case can't be finished. I am instructed to oppose it because there is one very important element and that is this question of the commission ...[indistinct] So we couldn't have adduced it before, M'Lord. So, in effect, the net result of it will be - the prejudice, M'Lord, is this. The prejudice is that it will delay the commission by probably - whatever period it is for us to resume this hearing and to complete the evidence in South Africa.

I have experts and witnesses because the witnesses are not all resident in Natal, who have had to fly down and be present and certainly, M'Lord, I can't ask, because a lot of them are expert witnesses at this point, until they qualify, M'Lord, I am unable to recover any costs in relation to them, and ...[intervention]

LEVINSOHN J Well, you may well be able to on the basis of an attorney and client charge.

MR LANE Yes, if there was an attorney and client charge for the wasted costs, M'Lord, including the costs ...[intervention]

LEVINSOHN J With respect to the witnesses that have flown from Johannesburg and come back and inevitably they would have - well, would you have been in a position to start with your case?

MR LANE Yes, M'Lord. I have both factual witnesses, M'Lord ...[intervention]

LEVINSOHN J Yes, I think you would have.

MR LANE Yes, M'Lord, I have both factual witnesses and expert witnesses, all, as Your Lordship has seen in court, I have a - as was referred to in ...[indistinct]... a gaggle of experts.

LEVINSOHN J Yes, it's almost like War and Peace.

MR LANE Yes. So, M'Lord, I could have begun indeed and the only way we would be compensated is if we had some special order to cover the costs of having to bring them back again.

LEVINSOHN J Yes. Mr Kissoon Singh, you are asking for an indulgence and there is this element of wasted costs here. That's pretty ...[intervention]

MR KISSOON SINGH It's not likely to have finished in the box

tomorrow in any event.

LEVINSOHN J You see, the hypothesis is this. You would have closed your case and he would have started his case ...[intervention]

MR KISSOON SINGH M'Lord, no, not ...[intervention]

LEVINSOHN J I beg your pardon?

MR KISSOON SINGH I said not necessarily, M'Lord, because there would still be an argument about whether he's entitled to lead evidence in rebuttal.

LEVINSOHN J I see. You are going to challenge that?

MR KISSOON SINGH Yes, M'Lord, I made that quite clear all along.

LEVINSOHN J Yes, I know you did, yes.

MR KISSOON SINGH And, M'Lord, in any event, I would have to ask M'Lord for the indulgence to allow the matter stand down to call various other lay witnesses whose evidence might not follow at a logical sequence at this particular point in time, such as the person who got married at the wedding which M'Lord has heard that the defendant attended over the week-end of the 4th and 5th. She has just arrived from Stanger, M'Lord.

LEVINSOHN J You mean in support of his alibi?

MR KISSOON SINGH Well, M'Lord, in support of saying that he wasn't overseas at the time. And, M'Lord, there's the driver who would give evidence ...[intervention]

LEVINSOHN J Of the hijacking?

MR KISSOON SINGH That's correct, and that he was here on the Monday morning. So it's not necessarily so that the case would close immediately if M'Lord were to refuse the adjournment.

LEVINSOHN J Mr Lane, well, my attitude is that, while I have some sympathy for your client, I would be disposed to reserve those costs and perhaps see how the case unfolds and whether you would be entitled inevitably to get these wasted costs. I imagine that you would be but I'm not in a position really to decide it now.

MR LANE This is a concern, M'Lord, and, in fact, I rather foreshadowed Your Lordship's attitude when taking instructions on this matter that it would ultimately possibly be that we would have to look at a reserved order if the matter did not proceed, for that very problem, M'Lord.

LEVINSOHN J Yes, I would reserve the issue of the wasted costs occasioned by the qualifying, because they might have to qualify themselves again, they have to reread all the material and they've got to travel again and they've got to be put up again.

MR LANE That is so, M'Lord.

LEVINSOHN J So I'd reserve all those costs.

MR LANE . Yes, M'Lord, and then would you give an order in relation to the balance of the costs? Just the ordinary wasted costs, just reserve those in relation to the witnesses that have travelled, M'Lord.

LEVINSOHN J I would reserve the costs of your witnesses that have travelled. What do I say, just the wasted costs occasioned - just try and formulate it. I just formulated it, this is just cobbling something together quickly, just see if you find this suitable. I would first of all make a blanket order that the case be adjourned subject to the defendants paying the wasted costs occasioned by the adjournment and, more particularly I would reserve for decision by me at the end

of the trial the wasted costs of the witnesses - that's the non-expert witnesses - who have travelled to be present at court during the course of this trial and, secondly, the qualifying fees of all experts, including their travel and the subsistence accommodation of such witnesses.

MR LANE Just one other aspect, M'Lord, it will obviously be necessary to get a transcription of the record.

LEVINSOHN J Well, that will be in the cause. That usually is in the cause.

MR LANE Shared by the parties and in the cause, M'Lord.

LEVINSOHN J And it becomes a costs factor - the parties now share it and then thereafter the winner gets the costs of that.

MR LANE Yes, M'Lord, that is understood. The only other aspect I'm asked to ask Your Lordship is as to when one might be able to resume this matter.

LEVINSOHN J What I propose to do is to direct that the Registrar use her best endeavours to place this matter on the roll for June when I'm here because I think thereafter there might be some difficulties.

MR LANE As Your Lordship pleases.

LEVINSOHN J Mr Kissoon Singh, any problem with any of this?

MR KISSOON SINGH No, M'Lord. June is fine but not May because I will be otherwise occupied on the Bench in May myself, but June will be fine.

- -

ORDER 7 MARCH 2002

LEVINSOHN J Very well, I adjourn this case to a date to be arranged and I direct that the Registrar place this matter on the roll during the month of June when I am on duty in Durban.

I direct that the defendants jointly and severally pay the wasted costs occasioned by the adjournment of the trial at 11.45 on the 7th March 2002. This order for wasted costs is subject, however, to the reservation of the following items of costs,

(1) The wasted costs occasioned by the plaintiff's witnesses who have travelled to be present in court during the course of this trial and,

(2) The qualifying fees and the travelling and subsistence expenses of all experts who have been present in court and have not given evidence.

All these aspects of the matter will be reserved for decision by me when the case is finally disposed of.

- -

MR LANE As the Court pleases.

MR KISSOON SINGH As the Court pleases.

LEVINSOHN J Yes, very well.

COURT ADJOURNED *SINE DIE*

TRANSCRIBER'S CERTIFICATE

I, the undersigned, hereby certify that so far as it is audible, the foregoing is a true and correct transcription of the proceedings recorded by means of a mechanical recorder in the matter of:

DINERS CLUB v A SINGH & ANOTHER

CASE NO	:	3156/00
COURT OF ORIGIN	:	HIGH COURT, DURBAN
TRANSCRIBER	:	N BINEDELL
No of Tapes	:	CD
Number of Pages	:	338

SNELLER RECORDINGS (PTY) LTD
DURBAN
TEL:- 031-2665452
FAX:- 031-2665459