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:-

PC.

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.

PL.

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.

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.

PG.

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.

I.G.

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.

P.6.

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.G.

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.G.

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

P.G.

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.

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.

P.G.

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

P.G.

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.L.

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

PG.

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).

PG

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.

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.G.

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.G.

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.

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

P Ca.

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

P.G. ~~17th~~ 20th day of ~~June~~ September, the regulations pertaining to the commissioning of such Affidavits having been complied with.

P.G.

COMMISSIONER OF OATHS P. Gittins

FULL NAME: PAUL GITTINS

BUSINESS ADDRESS:

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