Ross Anderson, FIEE, FIMA
Reader, Security Engineering

Master Turner
Queen's Bench Division
Royal Courts of Justice
Strand
London WC2A 2LL
Fax: 020 7947 7339

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

February 19, 2003

Dear Master Turner,

Diners Club (SA) Pty Ltd v Anil and Vanita Singh

I have been asked to act as a defence expert witness in the matter Diners Club SA (Pty) Ltd vs Mr A and Mrs V Singh, which I understand will come before you in chambers tomorrow. My research students Michael Bond and Richard Clayton have also been asked to act as defence experts. Our evidence is due to be heard by Mr Justice Levinsohn of the High Court of South Africa from 3-14 March 2003.

I was informed on Monday by the defence attorneys of an application before you on the 20th February for 'relief in relation to the protection of information which they accept as being confidential and which ought not to be in the public domain.' No further information was available then. This morning, I have received a fax with some case papers, including a draft order apparently sought by the group of companies including Citibank and Diners UK ('the Applicant') ordering that we attend; that the hearing be in camera; that the parties keep confidential all information revealed during the examination; that such information be used for no other purpose, and that the applicant's staff be exempted from testifying about the security of its systems.

It is of course quite proper for the applicant to ask you for an order protecting the confidentiality of any testimony by its exployees that reveals information whose publication would materially impair the security of its computer systems.

However, there are a number of problems with the much wider order actually sought.

First, my student Richard Clayton is travelling overseas on the 3rd and 4th March, and is in any case due to be called after my evidence and Bond's. An order compelling him to attend from the 3rd would be disruptive and is not legitimately justified. We three defence experts are attending the Court voluntarily and there is no need for compulsion.

Second, the terms of the secrecy order sought by the Applicant are oppressive. If granted, it would

Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD
England

Tel: +44 1223 334733
Fax: +44 1223 334678
E-mail: Ross.Anderson@cl.cam.ac.uk

interfere with my research, with my teaching, and with my ability to act as an expert in other matters.

My field of expertise is security engineering, which is about building systems to remain dependable in the face of malice, error or mischance. I am the author of many of the refereed scientific papers relating to the use of cryptography to protect networks of automatic teller machines (ATMs). From time to time, there are epidemics of fraud from ATMs, and one appears to be building now.

In the present matter, the defendants' case is that they had over £50,000 withdrawn from their Diners' Club card account by persons unknown who appear to have made 190 transactions at British ATMs in the first weekend in March 2000. At the time, they were in South Africa where they live. The essence of Diners' case is a claim that all the computer systems involved are secure, so the defendants must be responsible for the withdrawals. Both the plaintiffs and the defendants engaged expert witnesses. We both, independently, discovered gaping vulnerabilities in the design of the cryptographic equipment used by the applicants and by other banks involved. The applicant now seems to be asking you to prohibit public disclosure or discussion of these vulnerabilities.

However, the vulnerabilities in question are of significant scientific interest and are relevant to public policy. They have already been widely published and even incorporated into undergraduate teaching for an examined course here at Cambridge.

In October last year, my research student Mike Bond sent off a scientific paper for publication describing some of these vulnerabilities. This paper is published as Cambridge University Computer Laboratory Technical report no. 560, available from `http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf`. Shortly thereafter, but before Bond's paper appeared in public, a talk on another subset of these vulnerabilities was given at the RSA conference in Paris by one Mr Jolyon Clulow, then an employee of PRISM, a consulting firm engaged as experts in this matter by the plaintiff. Clulow subsequently discussed the vulnerabilities in a seminar he gave here in Cambridge on the 15th October last year; see `http://www.cl.cam.ac.uk/Research/Security/seminars/2002/2002-10-15.html`. Our discovery of the vulnerabilities followed perusal of case papers filed by the plaintiff in South Africa for which no order of confidentiality was ever sought or made; it was verified by reference to equipment manuals that are openly available (a point which the plaintiff has argued when claiming the relevant systems are secure). Some of the vulnerabilities were further verified by tests conducted in our laboratory on one of the affected types of machine.

As time passed, it became clear that the vulnerabilities were of much wider interest to computer scientists interested in cryptographic protocols. Bond and I wrote a paper which was delivered at a conference to celebrate the 50 years spent in Cambridge by Professor Roger Needham, the founder of this field of study. The paper has appeared in the proceedings of this event which are available online at `http://research.microsoft.com/~aherbert/volume63.pdf`. I also gave a talk on them in the security course that I teach for Part 2 of the Computer Science Tripos.

Bond plans to incorporate much of this material into his PhD thesis, which he is due to write up this year. It is spectacularly inappropriate for the applicant to ask you, in effect, to prohibit Bond from including in his thesis a scientific discovery that he has already published.

In addition to being published material, derived from open sources, and of crucial importance to the defendants' case, the vulnerabilities are likely to be crucially important in other cases brought in the UK and elsewhere over disputed transactions from ATMs.

I have acted as an expert witness in a number of civil and criminal matters relating to disputed ATM withdrawals over the last ten years. I have helped both banks and bank customers investigate problems; in fact, in 1994 I advised the Applicant. In criminal matters I have acted for both the prosecution and the defence. An order preventing public reference to the failings of particular commercial cryptographic systems would not merely impede the progress of science and engineering. It would also prejudice future litigants, future prosecutions and the rights of defendants in future criminal trials. It may even promote crime, by suppressing public domain information needed to motivate upgrades to ATM security. Thus an order in the terms sought by the Applicant – preventing us from using information arising in the course

of our testimony for any other purpose – would have a significant adverse effect on the administration of justice in the UK, and elsewhere. I respectfully submit that such an order would be profoundly contrary to public policy, as well as the Human Rights Act.

Third, the defence experts are being called first and the plaintiff's witnesses second at the hearing on the 3-14 March 2003 . This may seem odd, but as I understand it the Court in South Africa accepted a certificate of indebtedness as the plaintiff's case, then left it to the defence to challenge that by raising issues about the correctness of the debits. The effect is that during the first week of the hearing, my students and I will be giving evidence on the lack of security of the applicants' systems as described in expert notices already filed in open court and without any application or order for confidentiality. Thereafter, I understand, the plaintiff seeks to call the applicant's current and past employees to rebut this evidence. Our evidence is based wholly on open source material, and its most embarrassing parts (from the applicant's viewpoint) have already been widely published. There is no privileged information from the applicant, or so far as I am aware from anywhere else, that has contributed to the testimony we will give.

Under the circumstances, I respectfully submit that it would not be reasonable or legitimately justified to make any secrecy order at all concerning defence expert testimony.

Fourth, I take no view on the dispute before you between the plaintiff and the applicant on whether the former may call the latter's staff to give rebuttal evidence. I obviously have no objection to your granting an order protecting the confidentiality of any testimony by the applicant's exployees that reveals information whose publication would materially impair the security of its computer systems. However, I would point out that much of the detailed information for which relief is sought in the draft order is already in the public domain. IT standards for ATM systems are largely public; the architecture of the relevant systems of the applicant has already been described in expert notices; the use of cryptography to deal with PINs has been the subject of academic publication since the 1970s, with the early papers (and one reference book) written by IBM engineers who developed the system currently in use; and the generic attacks possible against computer systems are the subject of intensive and widely published research.

Fifth, much of the remaining information for which protection is sought is relevant to the defendants' case. For example, the physical location of DCI's PIN processing was claimed by the applicant's expert notices to be in Farnborough, Hampshire, but by the plaintiff to be in Germany. I suggest that the information whose protection is sought at 2 (ii) and (vi) of the draft notice thus relates more to the truthfulness of witnesses than to the protection of the applicant's installations against mail interception attack as suggested by Mr Teichgraeber.

I am unable to attend the hearing tomorrow as I am lecturing and hosting an overseas guest at a seminar here in Cambridge. The defendants in the South African case are of limited means and are unable to brief British lawyers to appear before you.

I am therefore writing to request you to not grant a secrecy order wider than is strictly necessary. In particular, I respectfully submit that no secrecy order should be granted against defence witnesses, except a duty not to repeat any new and clearly confidential information offered by the applicant's current and former staff while testifying as the plaintiff's rebuttal witnesses.

An order in the terms sought by the applicant would be inappropriate in the extreme. It would suppress scientific research and teaching, and it would undermine the rights of the many other victims of the current wave of 'phantom withdrawals' from cash machines. Tt would also needlessly interefere with the administrative arrangements being made by defence witnesses to testify at the hearing in March.

Yours sincerely,

Ross Anderson