Published in issue 123 of the Journal of the British Insurance Lawyers Association

JustCard plc v Cybersafe Ltd mock trial: judgment

By Sir Richard Aikens

Note: this "judgment" is not to be regarded as an official view on either the facts or the construction of the terms considered. For the background to the mock trial see the article by Laura Crowley at page 31.

1. This a claim on a policy called a cyber protection policy which came into effect on 1 January 2011 for 12 months. The claimant is JustCard plc, which is a small pre-paid card processing business. It uses its own processing system called "ProcessSys". The defendant, the insurer, is Cybersafe Ltd, who wrote this policy through their underwriter, Mr. Frye, who gave evidence before me.

2. There was a cyber attack on JustCard's system in February 2011. As a result unauthorised ATM withdrawals totalling £15.8 million were made. This attack occurred by means of 10,000 individual withdrawals in some 30 countries. The underwriters were notified of these unauthorised withdrawals very soon thereafter. The system, ProcessSys, was shut down. Lawyers, public relations consultants and an information systems specialist were appointed by the assured to conduct an investigation into the system, the company's infrastructure and all the processes. The clients of JustCard had their accounts reimbursed with all their losses within a matter of 3 days.

3. However, JustCard claim losses totalling some £73 million. They say that the initial fraud losses were those represented by the repayments that they had to make to the customer accounts. They say they incurred "crisis management" costs of £24 million. There were other costs under 3 heads of £26, £5 and £3 million respectively which I need not detail.

4. The defences to the claim are these: first it is said that there was non-disclosure of material facts. Secondly it is said that Exclusion 2A of the policy applies to exclude all liability.

5. If those defences fail then underwriters have two defences in relation to two particular claims. First, they say that the initial fraud losses are not within the terms of the insuring agreement 3. Secondly, they say that the crisis management costs are not within the terms of insuring agreement 6. Those are the relevant insuring agreement terms under which those particular claims have been made.

6. I heard evidence from two witnesses on behalf of the claimant. They were Miss Hancock, who is the CEO of the claimant, and Glenda Avery, who is the risks manager. They gave their evidence clearly and concisely. I am satisfied that they were telling the truth.

7. I heard evidence from Mr. Frye, the underwriter. I am satisfied that in general terms

he also gave clear, concise and truthful evidence. There is, however, one respect in which his evidence under cross-examination did not accord with that which he gave in his witness statement. In his witness statement, paragraph 9, he says that had he been told in December 2010 that JustCard had not upgraded its software to edition 3.17 "….I would have required as a condition of cover that this upgrade be installed because out of date security protection materially increases the risk of a cyber attack being successful". When he gave answers to the questions in cross-examination he said that he did not ask about upgrades, but he did not do so because it was not in his thinking at the time.

8. The basis for the non-disclosure defence is that the underwriters were not told about the fact that JustCard had decided, for entirely commercial reasons, that they would not upgrade the software for their system because it was going to cost them £2 million to do so. Miss Hancock was frank in saying that under normal circumstances she would have wished to have upgraded to the system 3.17 and that she recognised that upgrades were needed to prevent attacks by hackers. Similarly Miss Avery accepted in cross-examination that, from a pure security perspective, un upgrade should have been made.

9. In my judgment there is no doubt that the fact that the assured had made this decision not to take the upgrade is a material fact. It is something which a prudent underwriter would want to know and it is a question that the prudent underwriter would be interested in for the purposes of this type of insurance. However, I am not convinced, having heard Mr. Frye, and seen him in the witness box, that he was influenced by this non-disclosure and in any sense "induced" by the non-disclosure of the decision not to up-grade to enter into the insurance. That is because, it seems to me, the evidence that he gave in the witness box more accurately reflected his position as underwriter, at the time that the risk was written, than that which is said in the carefully crafted paragraph 9 of his witness statement.

10. Accordingly I am not satisfied that the non-disclosure defence succeeds.

11. I turn then to Exclusion 2A. This exclusion will only be of assistance to the underwriters if it can be established that any claim was "directly or indirectly arising out of or attributable to the failure to use best efforts to install commercially available software product updates and releases". So far as the second part of that quotation from the exclusion wording is concerned, I am satisfied that the assured used no efforts whatsoever to use commercially available product updates. Indeed they made a positive decision not to do so.

12. The key question, therefore, is whether or not any claim "directly or indirectly arises" out of the fact that the assured made no effort to install commercially available software product updates and releases. The argument of the insurers is that, on the facts, if the update had been installed the type of attack which was in fact used would have been

prevented. However, it is, I find, clear that cyber attackers could have used other methods which would have been successful. So the question is whether or not the opening words "We shall not be liable for any claim directly or indirectly arising out of or attributable to the failure …" means that in this case there is no cover, or rather cover is excluded.

13. I have come to the conclusion that this exclusion does operate in favour of the insurers. This is because the exclusion must relate to the particular claim with which the insurers are faced. Any claim cannot just be put in the abstract. This is a claim based on this particular type of cyber attack and the particular methods that were in fact used by the attackers. That attack and those methods would have been prevented if those best efforts have been used by the assured to install the up to date software.

14. I find, therefore, that this claim is excluded in total. I will, however, go on briefly to deal with the two further matters which were argued before me.

15. I should say that the argument, and indeed the presentation of the case generally, and the handling of the witnesses were all accomplished with considerable expertise and dispatch by all counsel, to whom I am extremely grateful.

16. I deal first, then, with the question whether or not, had there been cover, there would have been a right to be indemnified in respect of the costs to the assured of reimbursing the client accounts. This depends upon the correct construction of insuring agreement 3. It states that the insurers will pay on behalf of the assured all damages which the assured becomes legally obliged to pay as a result of any claim made against the assured as a result of one of the insured events.

17. The problem for the claimants is that there is no loss that was incurred by the clients and there are no damages which the assured have become legally obliged to pay. The position was, before the attack, that the assured were debtors of their clients to the extent of the credit on each of their clients' accounts. That remained precisely the position after the attack. The fact that there was a cyber attack made no difference to the position as between the assured and their clients; the first was the debtor of the second.

18. So, in my opinion, the reimbursement of the client accounts is not a claim which falls within the terms of the cover. There is no claim for damages that a client has made against the assured as a result of an insured event. In any event there has been no "claim" within the definition of that phrase in the policy. Accordingly I would have, in any event, rejected that claim.

19. The second head of claim that is in question is the claim for crisis management costs. Here the boot is on the other foot. The underwriters say that before there can be any liability, the crisis management costs that are claimed have to have been approved by them before the costs are incurred. For this purpose they rely upon the definition of crisis management costs at page 9 of the policy wording.

20. I cannot accept that argument. In my view the correct construction of insuring agreement 6 is that there is a liability for crisis management costs as a type of expense, provided that those have been incurred following a security breach and provided that the security breach has been notified by the assured in writing to the underwriter, in accordance with the policy terms.

21. It is only when one turns to the question of "how much crisis management costs?" that the definition of that term becomes relevant. And it is in those circumstances that the assured can only recover any fees reasonably incurred by him, which fees have been approved by underwriters, i.e. at the point when questions of quantum arise. Those fees have to have been incurred for the purpose of the employment of a public relations consultant, etc.

22. I do not accept the argument that "approved by us" means that there has to be prior approval before liability can even be incurred. If it was such a pre-condition one would expect it to be in clear terms in the insuring agreement clause. It is not.

23. Accordingly I would have accepted that there was liability in principle for such costs. This hearing, however is not dealing with quantum, so I have no need to go into that in any event.

24. But, as I have already indicated, in fact the underwriters succeed in their defence on the exclusion clause. Therefore this claim must fail.

Sir Richard Aikens is a Lord Justice in the Court of Appeal and the deputy president of BILA. His participation in the cyber risk mock trial was in an unofficial capacity.