

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
COMMERCIAL COURT

B E T W E E N:-

JUSTCARD PLC

Claimant

- and -

CYBERSAFE LTD

Defendant

CLAIMANT'S SKELETON ARGUMENT

1. The Claimant ("JustCard") has a policy of insurance ("the Policy") with the Defendant ("Cybersafe") which came into effect on 1 January 2011 for 12 months. Its intention was to indemnify JustCard against losses arising out of cyber attacks. At the end of January 2011 JustCard was the victim of a cyber attack, causing it significant losses. This action is necessary because Cybersafe is seeking to avoid its obligation to indemnify JustCard against its losses.
2. This skeleton argument addresses the following issues:
 - 2.1. Did JustCard's failure to disclose the fact that it had not upgraded ProcessSys amount to a material fact which entitled Cybasafe to avoid cover?
 - 2.2. Are Cybersafe entitled to exclude the claim because it arises out of a failure on the part of JustCard to use best efforts to install commercially available software product updates and releases?
 - 2.3. If there is cover, does it cover:
 - 2.3.1. The initial fraud losses?
 - 2.3.2. The crisis management costs?

Issue 1: Avoidance?

3. In November 2010 an upgrade for ProcessSys was released, which JustCard did not purchase for budgetary reasons.¹ Cybersafe allege JustCard should have told Cybersafe's underwriter. JustCard denies that it needed to tell Cybersafe about the lack of upgrade, because it was not material to the risk; alternatively, if it was, Cybersafe waived any need for disclosure.

¹ Hancock §4; Avery §4.

The presentation of the risk

4. The risk was written by Mr Frye after a presentation by Mr Jarvis, JustCard's broker. Mr Frye did not ask for a proposal form to be completed. Nor did he ask for an expert review of JustCard's software. He simply relied upon documents presented by Mr Jarvis. Mr Frye was aware of ProcessSys, and knew that it "*was among some of the most advanced software in guarding against cyber attacks.*" He assumed that it was up to date.²

The basic legal principle

5. It is well established that the insured must disclose to the insurer before the risk is written every fact which is material to the risk. A fact is material if it would influence the judgment of a prudent insurer in fixing the premium or other terms, or determining whether he will take the risk. If the insured fails to disclose a material fact, and if the non-disclosure of the material fact induced the insurer to enter into the contract on the relevant terms, then the insurer will be entitled to avoid the insurance contract.³

Was the presentation fair?

6. In this case, the presentation of the risk was fair. Mr Jarvis gave Mr Frye full details of the relevant software. Mr Frye understood that the software was up to date in accordance with Cyber Security Guidance version 3.16: that was accurate. Mr Frye is by his own admission immensely experienced in this type of business and felt able to make his own appraisal of the security system without the need for independent specialist advice. He "assumed" that it was the most up to date version of the software, but that was his assumption. It was not because he had been told that it was the most up to date software. The software was relatively new, and well thought of: Mr Frye knew that. If it was important to him that the software should be the very most up to date version, then he should have asked about it.

Waiver

7. An insurer is not entitled to avoid for non disclosure where he was sufficiently put on enquiry of a point, but failed to ask any questions about it.⁴ In such circumstances, the insurer, having waived the opportunity to ask further questions, may not complain that he was not given further answers. That does not extend to undisclosed facts which are unusual or special⁵. The issue is whether the insurer has been put on inquiry and has nevertheless refrained from asking further questions.⁶
8. In this case, there can be no suggestion that the availability of upgrades is unusual or special. Indeed, the Exclusion Clause presupposes them. Mr Frye assumed, he says, that the software was the most up to date version. That was not an assumption for which the insured was responsible. If, having been given full information about the software, it was important to him that the software was the most up to date version, he

² Frye §4

³ Section 18 of the Marine Insurance Act 1906; Pan Atlantic Insurance Co Ltd v Pine Top Insurance Co Ltd [1995] 1 AC 501

⁴ CTI v Oceanus Mutual Underwriting Association (Bermuda) [1984] 1 Lloyd's Rep 476, 496-7 per Kerr LJ

⁵ *CTI* at 498, per Kerr LJ.

⁶ See *Good Faith and Insurance Contracts* (MacDonald Eggers, Picken & Foss) (3rd Ed 2010) paragraph 8.59 discussing the decision of the Court of Appeal in WISE (Underwriting Agency) Ltd v Grupo Nacional Provincial SA [2004] EWCA Civ 962; [2004] 2 Lloyd's Rep 483

should have asked for confirmation. Having not done so, he cannot now turn around and complain that his assumption was wrong.

Not material

9. Further, the issue of whether or not the software was the most up to date version was not material to the risk, because any loss caused by the fact that the software was not the most up to date version was excluded by exclusion clause 2A.1 ("the Exclusion Clause").

10. The Exclusion Clause reads as follows:

We shall not be liable for any claim directly or indirectly arising out of or in any way attributable to ...

2A1. *the failure of Computer Systems or Data Assets to be protected by Computer Security equal to or superior to that disclosed in response to specific questions in the Application for Insurance relating to Computer Security, including access protection, intrusion detection, data back up procedures, Malicious Code protection, software product updates and releases, path protection, and data encryption; or*

2A2. *the failure to use best efforts to install commercially available software product updates and releases, or to apply security related software patches, to computers and other components of the Insured Organization's Computer Systems.*

11. An express warranty may displace an obligation to disclose a fact, when the relevant is adequately addressed by the warranty⁷. Similarly, it must follow that if a specific issue is dealt with by an exclusion clause, it is not material to the risk, because any risk arising from the issue has been avoided.

12. *Ex hypothesi*, if a loss were caused by a breach of the terms of the exclusion, it would be excluded; if it were not so caused, the fact that the software was not the most up to date version made no difference to insurers' liability and so was immaterial. Accordingly, whether or not the software was the most up to date version made no difference to insurers' liability.

Issue 2: the Exclusion Clause

13. Cybersafe seeks to argue that the loss is excluded by the Exclusion Clause. But that fails on the facts, because as a matter of fact, JustCard were not in "breach" of the terms of the clause and further because the loss was not caused by any failure on the part of JustCard "*to use best efforts to install commercially available software product updates and releases*".

14. In this case, the Systems and Data Assets were protected by Computer Security "equal to that disclosed in response to specific questions in the Application for Insurance" within the meaning of Exclusion 2A1.

⁷ Inversiones Manria v Sphere Drake Insurance Co Plc ("The Dora") [1989] 1 Lloyd's Rep 69, 91-92 per Philips J (as he then was).

15. Further, Exclusion 2A2 does not require as an absolute obligation that the most recent updates and releases shall have been installed but only that the Insured shall have used “best efforts” in that regard. The expression “best efforts” must be looked at in a business context and should not be interpreted as requiring an insured to install, at uncommercial cost, upgrades to a very modern system which it reasonably in all the circumstances decides not to purchase. Accordingly, the insured was not in breach of the Exclusion Clause on the facts of his case.
16. As to causation, the evidence establishes that (1) the mechanics of the cyber attack that took place would have been prevented by the up to date version of the software but (2) the cyber attack would be likely to have happened anyway, because SpookNet could have got around the upgrade: "*version 3.17 was not a material improvement on version 3.16*"⁸.
17. Plainly, one proximate cause of the loss was the cyber attack itself: that is an insured peril. It is now well established that if there are two proximate causes, one of which was covered and the other which is specifically excepted, the loss is not recoverable.⁹ So the question is whether the fact that the software was not the latest edition was a proximate cause of the loss. In those circumstances, it is fruitful in this particular case to consider the application of a "but for" test. Had the software been the latest version, would the cyber attack still have occurred? The answer, on the balance of probabilities, is yes. SpookNet might have had to carry out in a slightly different way, but having decided to attack JustCard, that is what they would have done.
18. The "but for" test is usually a necessary but not sufficient causal test¹⁰. Since Cybersafe cannot satisfy it in this case, the Exclusion Clause does not bite, and the claim should succeed.

Issue 3: the initial fraud losses

19. JustCard were obliged to reimburse customers for sums taken from their accounts, because the withdrawals were not authorised.
20. Pursuant to insuring agreement 3, insurers are obliged to pay **damages** (as defined) which JustCard became legally obliged to pay as a result of any **claim** (again, as defined) first made within the period of cover. The idea of being legally liable to pay damages may well include, in the context of a policy of liability insurance, sums which a party has a legal responsibility to pay.¹¹
21. Cybersafe suggests that the loss is not that of customers, but that of JustCard, and there is no cover for losses suffered solely by JustCard (outside the recovery of costs and expenses under insuring clause 4). That is a submission which is overly legalistic and unrealistic, whilst at the same time also being legally inaccurate. The customers did suffer a loss, in that the debt owed to them by JustCard by way of their account balance had been reduced for a period of time by reason of the cyber attack. The fact

⁸ Rolland §8.

⁹ Wayne Tank and Pump Co Ltd v Employers Liability Assurance Corporation Ltd [1974] QB 57, 75; Global Process Systems v Syarikat Takaful Malaysia Berhad (the "Cendor Mopu")[2011] UKSC 5; [2011] 1 Lloyd's Rep 560, § 22 and §88.

¹⁰ Orient-Express Hotels Limited v Assicurazioni General S.p.A. [2010] EWHC 1186 (Comm) §33 per Hamblen J.

¹¹ See, in a different context, but to similar effect, Bedfordshire Police Authority v Constable [2009] EWCA Civ 64, [2009] Lloyd's Rep. I.R. 607

that the balances were made good before most of them realised they had suffered a loss does not mean that they had suffered no loss for a period of time.

22. Cybersafe then argues that if there was a loss, the customer made no claim, because JustCard had already indemnified them.
23. The problem with this submission is that it fails on the wording of Cybersafe's own policy document. The word "claim" is defined in wide terms, including "**first party insured event**", which in turn is defined as loss sustained by JustCard arising from (among other things) a security breach, malicious code; and/or unauthorised use of JustCard's computer network.
24. Further or alternatively, the word "claim" also includes a "**crisis management event**"¹² or the incurring of "**customer notification expenses**"¹³ or "**customer support and credit monitoring expenses**"¹⁴. Each of those events had occurred, so as to give rise to a claim for the purposes of the Policy. More expansively, the wide definition of "claim" to this effect indicates that the parties undoubtedly intended that the Policy should respond to liabilities that might have to be satisfied by taking proactive steps, rather than sitting back and waiting for the complaints to flood in.
25. Yet further or alternatively, "claim" includes "Notice by a third party to **you** of circumstances that could reasonably be expected to result in any of the foregoing (i) to (v) above." JustCard was, of course, given notice of such circumstances by a third party - it does not really matter by whom - and they could undoubtedly have given rise to such events.
26. In short, the suggestion that there was no claim fails under the wording of the Policy. But the point can be taken further. Had JustCard not immediately repaid the sums to customers, there can be no doubt that each customer would have had a valid claim, which JustCard would have had to pay. In those premises, there can be no doubt that JustCard would be able to recover under the Policy. Is it to be penalised for having complied with its legal obligations swiftly and properly rather than slowly and obdurately?
27. The answer, of course, is no. In considering this issue, some assistance can be found in previous cases where, by reason of regulatory or statutory compulsion, insured have been obliged to make good losses in the absence of a claim, and then seek to be indemnified from insurers on claims made policies. The Court will seek to uphold the basic commercial purpose of the policy.

¹² **Crisis management event** means any unpredictable **newsworthy event** that threatens material damage to any of **your** brands, which results in **you** incurring **crisis management costs**.

¹³ **Customer notification expenses** means those reasonable and necessary legal expenses, public relations expenses, postage expenses, and related advertising expenses incurred by **you** to comply with governmental privacy legislation mandating customer notification in the event of a **security breach, privacy breach**, or breach of **privacy regulations** that results in the compromise or potential compromise of personal information maintained by **you** or otherwise residing on a **computer network** operated by **you** or on **your** behalf.

¹⁴ **Customer support and credit monitoring expenses** means those reasonable expenses **you** incur for the provision of customer support activity, including the provision of credit file monitoring services and identity theft education and assistance in the event of a **privacy breach** that results in the compromise or potential compromise of personal information maintained by **you** or otherwise residing on a **computer network** operated by **you** or on **your** behalf.

28. So, for example, in *J Rothschild Assurance plc v Collyear* [1999] Lloyd's Rep. I.R. 6 Lautro and its successor, the PIA (the Personal Investment Authority), required their members to set up a review to investigate the pensions mis-selling problem, and to offer redress to all those investors who, as a result of such review, were shown to have been mis-sold a pension in breach of the applicable self-regulatory rules and to have suffered loss as a result. With rare exceptions, losses were made good without claims ever having been asserted. Insurers denied liability on that basis. Rix J, as he then was, held that where the customer accepted redress in line with the regulatory scheme, that was sufficient to amount to a claim for the purposes of the policy: underwriters knew the class of business they were writing, and the regulatory systems which applied to it, and therefore should have anticipated that the regulatory scheme might require offers of compensation to be made to customers who had not made any complaint.

Issue 4: crisis management costs

29. The evidence establishes that:
- 29.1. JustCard incurred crisis management costs without expressly having sought Cybersafe's consent;
 - 29.2. Any failure on the part of JustCard to obtain insurers' consent was unintentional;
 - 29.3. What JustCard did by way of crisis management was exemplary.
30. Insuring agreement number 7 provides:
- We shall indemnify you for crisis management costs, customer notification expenses, and customer support and credit monitoring expenses which exceed your excess when such costs and expenses are incurred, following a security breach, privacy breach or breach of privacy regulations, and notified by you to us in writing, in accordance with Section 11 of this policy, during the policy period or any extended reporting period, if applicable, provided that the security breach, privacy breach or breach of privacy regulations occurred on or after the retroactive date.**
31. The short answer to this contention, on the part of insurers, is that crisis management costs are not only covered where insurers have first given their consent. All that needs to happen is that costs are notified in writing in accordance with section 11. That has happened. Therefore there is an indemnity.
32. The definition of crisis management costs includes a provision that the costs shall be "approved by us". But it does not state that approval has to be prior to their being incurred. It must also be subject to an implied term that consent cannot be unreasonably withheld.¹⁵ There is no basis for saying that consent could reasonably have been withheld, and nothing in this point.

¹⁵ See, by analogy, the decision of Thomas J (as he then was) in *Poole Harbour Yacht Club v Excess Insurance Co Ltd* [2001] 1 Lloyd's Rep IR 580, 586.

Conclusion

33. Cybersafe must be kept to their promise to indemnify. Their legalistic submissions should be rejected in their entirety. JustCard requests judgment in the sum of £73m plus interest.

MICHAEL DOUGLAS Q.C.
JAMES LEABEATER

4 Pump Court
Temple
London EC4Y 7AN

20 June 2011