British Insurance Law Association


**British Insurance Law Association (BILA) in association with The Professional Liability Underwriting Society (PLUS)**

**CYBER LIABILITY MOCK TRIAL**

**Wednesday June, 22, 2011**

**Cyber scenario – dramatis personae**

**The Policyholder :** **Just Card PLC**

**CEO:** **Marjorie Hancock …… Christine Williams**
**Risk Manager:** **Glenda Avery ……..Jacquetta Castle**

**The Broker:** **JPG Brokers**

**Placing:** **Derek Jarvis…….. Pat Donnelly**
**Claims:** **Marcus Edge …… David Nayler**

**The Insurance Company:** **Cybersafe Insurance**

**The Underwriter:** **Philip Frye…….. Rick Welsh**

**Information Systems Specialists: Rolland Dean**

**Director:** **Todd Rolland…… Ken Munro**

**Software Company:** **Software Solutions Ltd**

**Account representative: Rob**

**Cyber gang:** **SpookNet**

**Specialist IT law firm:** **Merrick & Brent LLP**

**Public relations consultant:** **Aterbury LLP**

**PLEASE NOTE THAT BADGES WILL BE SUPPLIED AND SHOULD BE WORN AT ALL TIMES – THIS IS A SECURITY REQUIREMENT AT THE ROYAL COURTS OF JUSTICE AND THE GARDENS AT GRAY'S INN**

British Insurance Law Association


**British Insurance Law Association (BILA) in association with The Professional Liability Underwriting Society (PLUS)**
**CYBER LIABILITY MOCK TRIAL**
**Wednesday June, 22, 2011**

**The Trial - – dramatis personae**

| | |
|---|---|
| **Presiding:** | **Rt Hon Lord Justice Aikens** |
| **Clerk:** | **Laura Crowley - 4 Pump Court** |

**Counsel for the Policyholder - Just Card Inc**

**Michael Douglas QC - 4 Pump Court**
**James Leabeater - 4 Pump Court**

**Counsel for the Insurance Company- Cybersafe Insurance**

**Tom Weitzman QC -3 Verulam Buildings**
**Nick Craig - 3 Verulam Buildings**

**Witnesses:**
**The Underwriter – Philip Frye**
**The Broker – Derek Jarvis**
**The Policyholder CEO – Marjorie Hancock**
**The Policyholder Risk Manager – Glenda Avery**
**The Expert Witness – Todd Rolland**

British Insurance Law Association

Professional Liability Underwriting Society PLUS the quintessential source of information and education on professional liability

**CYBER LIABILITY MOCK TRIAL**
**Wednesday June, 22, 2011**

**Offices of Freshfield Bruckhaus Deringer LLP, 65 Fleet Street, EC4Y 1HT**
**access is via the Tudor Street entrance see Directions**

| | | |
|---|---|---|
| **2.00 pm** | **Registration and refreshments** | |
| **2.30 pm** | **Welcome from Raj Parker, Partner, Freshfields Bruckhaus Deringer LLP** | |
| | **Introduction by Stephen Lewis, Clyde & Co, Chairman of the British Insurance Law Association** | |
| **2.40 pm** | **Presentation by Ken Munro of Pen Test Partners** | |
| **3.10 pm** | **Role play session on the mock trial scenario** | |
| | **Cyber requirements** | **Glenda Avery – Risk Manager of Just Card PLC**<br>**Derek Jarvis - of JPG Brokers** |
| | **Broking the Risk** | **Philip Frye - underwriter for Cybersafe**<br>**Derek Jarvis - of JPG Brokers** |
| | **The loss occurrence** | **Marjorie Hancock - CEO of Just Card PLC**<br>**Glenda Avery - Risk Manager of Just Card PLC** |
| | **The claim** | **Marjorie Hancock - CEO of Just Card PLC**<br>**Glenda Avery - Risk Manager of Just Card PLC**<br>**Marcus Edge– Claims Broker at JPG Brokers**<br>**Todd Rolland – Rolland Dean** |
| **3.35 pm** | **Break** | |
| **4.20 pm** | **End of part one** | |

**The event now moves to Court 4 in the Royal Courts of Justice, Strand, WC2A 2LL**

| | |
|---|---|
| **5.00 pm** | **The Mock Trial commences with** |
| | **The Rt Hon Lord Justice Aikens presiding**<br>**Laura Crowley - 4 Pump Court as Clerk to LJ Aikens** |
| | **Counsel for the Policyholder - Just Card PLC** |
| | **Michael Douglas QC - 4 Pump Court**<br>**James Leabeater - 4 Pump Court** |
| | **Counsel for the Insurance Company- Cybersafe** |
| | **Tom Weitzman QC - 3 Verulam Buildings**<br>**Nick Craig - 3 Verulam Buildings** |
| **7.00 pm** | **The Mock Trial ends** |

**Participants and delegates proceed to the Gardens of Gray's Inn, WC1R 5ET for**

| | |
|---|---|
| **7.30 pm** | **Garden Party – Drinks and Bar-B-Que** |
| **9.30 pm** | **The event closes** |

JUSTCARD -v- CYBERSAFE

1. Prepaid cards allow customers to make purchases and withdraw cash from a sum of money they have paid to the card provider. JustCard is a small pre-paid card processing business, with its own processing system called "ProcessSys".

2. On 1 February 2011 JustCard's Risk Manager, Glenda Avery, was informed that on 26, 27 and 28 January 2011 unauthorised ATM withdrawals totalling £15.8 million had been made. More than 10,000 individual withdrawals had been carried out using 50 counterfeit prepaid cards from over 2,100 ATMs in 30 countries.

3. Justcard was insured with Cybasafe pursuant to a Cyber Protection Policy for the period 1 January 2011 to 31 December 2011. The Risk Manager, Ms Avery, notified insurers of the unauthorised withdrawals on 2 February 2011 and this notification was accepted as valid.

4. ProcessSys was shut down immediately by Justcard. The sums which had been unlawfully withdrawn were all re-credited to cardholders' accounts by Justcard by 3 February 2011.

5. On 2 February 2011, Justcard instructed a law firm (Merrick & Brent LLP), a public relations consultant (Aterbury LLP) and an information systems specialist (Rolland Dean) to conduct a thorough investigation of their systems, infrastructure and processes. On advice from Merrick & Brent, it notified the police, the FSA, the Information Commissioner's Office and the Serious Organised Crime Agency of the fraud and, thereafter, gave all assistance that it could to the criminal investigation.

6. On advice from Merrick & Brent and Rolland Dean & Co, JustCard implemented the following remediation programme:

   - Containment steps: cancelling cards, contacting counterparties.

   - Enhanced security steps: significant work was carried out to enhance security, including applications, network, systems, databases, fraud management and IT staffing.

   - Future security model: rolling review plan and IT updates planned.

7. JustCard did not keep Cybasafe properly abreast of its remediation programme or the expenses that it was incurring in implementing it. In particular, it did not specifically advise or seek the express approval of Cybasafe before incurring any of the costs arising from its remediation programme. However, Justcard's swift and systematic response has avoided the risk of any further similar attack and has won plaudits from the relevant government agencies, reducing reputational damage.

8. Rolland Dean's investigations revealed that a cyber intruders gang, known as "SpookNet", had been able to exploit weaknesses in the security system. SpookNet had been able to obtain prepaid card data, manipulate card balances, and using

counterfeit cards withdraw the sums of money from ATMs. Whilst JustCard's systems were top of the range in 2009 when installed, better products had become available. The security system had been due to be upgraded in the autumn of 2010, but this had not been done for budgetary reasons. Had the upgrade been carried out, the attack could not have been made; however, the system would still have been vulnerable to attack and could still have been circumvented by SpookNet.

9. JustCard suffered losses of about £73m:

| | |
|---|---|
| Initial fraud losses | £15m |
| Crisis management (PR) | £24m |
| Recall of pre-paid cards | £26m |
| Long-term remediation | £5m |
| Other potential liabilities | £3m |

10. JustCard sought to be indemnified by Cybasafe to the full extent of its losses. Insurers declined cover for the following reasons:

10.1. In relation to the failure to upgrade the system in autumn 2010:

10.1.1. JustCard failed, at placement, to disclose the fact that it had not upgraded ProcessSys in line with the manufacturers' recommendations because it was too expensive. That was a non disclosure of a material fact which entitled Cybasafe to avoid cover.

10.1.2. Alternatively, the loss is excluded 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.

10.2. If there is cover, it does not extend to the initial fraud losses, because the customers themselves suffered no loss: monies had been re-credited to their accounts by Justcard without any claims being made.

10.3. If there is cover, it does not extend to the crisis management costs. The Cyber Safe Policy indemnifies against crisis management costs incurred with the prior approval of underwriters, but JustCard did not ask for approval before incurring costs.

11. JustCard have issued proceedings in the Commercial Court for a full indemnity under the Policy.

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

---

**WITNESS STATEMENT**
**OF GLENDA AVERY**

---

I, Glenda Avery, of JustCard Plc, Darwin Industrial Estate, Slough, Berkshire will state as follows:-

1. I am the Risk Manager for JustCard plc ("JustCard"). I am responsible for, among other things, arranging JustCard's insurance cover and its security systems. I have been employed in this role since September 2007.

**JustCard's Cyber Security System**

2. JustCard is a pre-paid card processing company. It is a relatively new company and its profits have been relatively modest over the past 5 years.

3. In 2008 I started discussions with a company called Software Solutions Limited for the development of a software system for its business. One of the things that I was concerned to ensure was that the system was sufficiently robust so that it could not be hacked. Software Solutions Limited developed a bespoke system which it called ProcessSys. JustCard started to use it in 2009. The security systems which formed part of it were extremely advanced. In fact, I understand that Software Solutions Limited won a number of awards for them as they marked a major advance in such systems.

4. ProcessSys did, however, cost JustCard a significant amount in money terms to develop and implement. In late 2010 Software Solutions Limited advised me that it had developed an upgrade to the security systems within ProcessSys to deal with the increasing sophistication of hackers. The cost of the upgrade was, though, in my view significant and, given how much JustCard had spent the previous year on the system. My chief executive, Marjorie Hancock, took the view that the company could not really afford it. We decided, particularly as the system had been developed at some significant expense to JustCard and been implemented only 12 months or so previously, not to purchase the upgrade.

**The Cybersafe Policy**

5. At about the same time that I declined to purchase the security system upgrade to ProcessSys I had my annual renewal meeting with Mr Jarvis of JPG Brokers. He suggested that JustCard should consider cover against cyber risks as cyber attacks or hacking was becoming more common.

6. I had a meeting with Mr Jarvis in the middle of November to discuss in greater detail the nature and scope of the cover and he supplied me with a copy of a document entitled Cybersafe Protection Policy (which I did not read). I explained to him the details of ProcessSys and provided him with a copy of the Operating Manual. I then consulted Ms Hancock, the chief executive of JustCard who authorised me to obtain quotations for such cover. Shortly after this, I instructed Mr Jarvis by telephone to obtain quotations.

7. Mr Jarvis reported back a couple of weeks later and advised that Cybersafe Limited had quoted as lead on the terms of the Cybersafe Protection Policy. I instructed him to place this cover and the insurance accordingly incepted with effect from 1 January 2011. I should make clear that I cannot now say whether I read the terms of the Cybersafe Protection Policy all the way through at the time. I suspect that I skim-read them, but since everything appeared to be in order, I probably did not spend too much time doing it.

**Crisis management costs**

8. On 1 February 2011 I was told that on 26, 27 and 28 January 2011 50 counterfeit prepaid cards had been used to withdraw a total of £15.8 million from ATMs in 30 countries; I learned that more than 10,000 individual withdrawals had been made at over 2,100 ATMs. I immediately put into action JustCard's disaster recovery plan. The first step in this process was to shut down ProcessSys and to re-credit those sums which had been unlawfully withdrawn to JustCard's customers. All such monies had been re-credited by 3 February 2011.

9. I notified JPG Brokers of the unauthorized withdrawals by letter dated 2 February 2011 and understand that this was passed on the Cybersafe Limited who accepted this notification as valid. I also informed the police who took the matter very seriously and, as I understand it, took steps to liaise with various law enforcement agencies worldwide. I received various requests for information from a number of such agencies and provided as much information as I could on each occasion as I was keen to assist in discovering the persons responsible for the fraud as well as in preventing such a fraud occurring again.

10. Acting closely with the CEO, Ms Hancock, I instructed Rolland Dean, the well known information systems specialists, to conduct a thorough investigation of JustCard's systems, infrastructures and processes and to attempt to determine the nature of the security breach which had occurred. I also instructed Merrick & Brent LLP, the well known specialist IT law firm, and Aterbury LLP, a public relations consultant. Each of these was, I understand it, one of the best in their relevant fields. The risk posed by the cyber attack to JustCard's business justified – indeed required – us to employ the very best.

11. Aterbury LLP acted very quickly to put into place a public relations briefing and thereafter to deal with the press internationally so as minimise the public relations

damage which I believe would otherwise have been caused to JustCard by reason of the counterfeit cards and the fraudulent withdrawals. In JustCard's business, public perception of security is paramount; if customers or potential customers do not believe that their money is secure with a particular company, they will not use that company. In fact, I would go so far as to say that without an effective public relations exercise following a security breach such as that which occurred with ProcessSys at the end of January 2011, the company concerned would cease to exist. Aterbury LLP were very effective in their public relations exercise and no major clients left JustCard as a consequence of the incident. It was, though, an exercise which had to be carried out quickly. We were, therefore, not able to obtain comparative quotations from other companies in this field. By reason of the fact that this exercise had to be conducted on an international scale it was very costly; the total bill for it was £24 million.

12. As I have said, I am not sure that I had read the policy in detail. Certainly on 1 and 2 February 2011, I was not consciously aware of the requirement that we should obtain underwriter's approval before incurring crisis management costs. I did not have the time to sit down and read the policy at the time and, in any event, our priority was to protect the business rather than thinking about the technicalities of our insurance claim. My experience of dealing with insurance companies leads me to suspect that had we asked underwriters for their permission to incur crisis management costs, they either would have taken some time to get back to us, so that we would have had to incur them in any event, or they would have replied with some relatively non-committal phrase such as 'we had an obligation to act as a prudent uninsured'. In my experience, it is unusual for underwriters expressly to agree to anything which might confirm a claim, at least in the short term. I think it would frankly be totally unfair if insurers were entitled to decline to cover this claim, when everybody seems to agree that what we did was necessary, reasonable and efficient.

**STATEMENT OF TRUTH**

I believe that the facts stated in this witness statement are true.

Signed: *Glenda Avery*

Dated 10 June 2011

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

---

**WITNESS STATEMENT**
**OF PHILIP FRYE**

---

I, Philip Frye, of Cybersafe Ltd, 132A Gracechurch Street, London EC3 will state as follows:-

1. I am an underwriter employed by Cybersafe Ltd, specialising in cyber risks cover. I have been writing this sort of risk since 2004 and, without being immodest, I think I am recognised as one of the most experienced underwriters in this particular market.

**Inception**

2. On 1 December 2010, Mr Jarvis of JPG came to see me to ask if I would quote for cyber risks cover for JustCard plc.

3. It is not my usual practice to ask brokers to complete proposal forms in relation to cyber risk cover, because the information I need to know is too detailed and complicated easily to be summarised in a proposal form. Rather, I ask to see documents relevant to the software systems used. In very complicated cases, I might instruct a specialist IT Consultant to review the security aspects of their software systems, so that I can rely upon an independent investigation before agreeing to write the risk. In this particular case, JustCard provided sufficient documentation and I therefore did not see the need for any such independent report.

4. Mr Jarvis, among other things, gave me a copy of the Operating Manual for the ProcessSys software, which had quite a lot of details about the security aspects of the software. I had, in fact, heard of ProcessSys because when it was first available it was among some of the most advanced software in guarding against cyber attacks. I noted that the software appeared to have incorporated provisions to deal with malicious attacks consistent with the Cyber Security Guidance version 3.16. All these types of software are constantly undergoing revisions and upgrades to improve them and, in particular, to make them more resistant to cyber attacks. I presumed that version 3.16 was the most up to date version of the software. On the basis of what I had been told about ProcessSys and JustCard generally, I agreed to quote as lead and gave Mr Jarvis my premium quotation, which was accepted. The policy was written on Cybersafe's standard terms.

**Crisis management costs**

5. I was informed of the cyber attack on, I think, 2 February 2011. On that day, I was attending a conference in Miami, Florida. However, I was able to read emails on my BlackBerry, and to take telephone calls in relation to this attack, which seemed to me to be relatively serious.

6. Although JustCard did notify me (through JPG Brokers) of the attack, they did not thereafter give any further details of what had occurred or the remedial steps that they put in place. I understand that they employed well-known public relations consultants, Aterbury LLP shortly after the attack and significant costs were incurred by them in "crisis management", namely seeking to limit the effects of publication of the attack in the media. However, I was never asked to approve any such costs either before they were incurred or at all.

7. It is my habitual practice carefully and promptly to consider requests for the approval of crisis management costs, because I recognise that it is of vital importance to my customers that crisis management policies are put in place as quickly as possible. Indeed, because of my experience in this particular area, I often find that I have some useful and constructive proposals to make. Unfortunately, I was not given the opportunity to do so in this particular case. The Policy requires that insureds seek underwriters' approval prior to incurring such costs, if they are to be recoverable, in order to ensure that the costs are sensibly and carefully targeted upon important issues. I have declined to pay this aspect of the claim precisely because the provisions are important and there appears to be simply no proper reason for JustCard to have ignored them.

**Inducement**

8. I understand that an update (ed. 3.17) was available for ProcessSys in November 2010 which JustCard chose not to purchase for financial reasons. Instead JustCard appear to have been happy to run the risk of an attack. I was not told about this at the time. Subsequently (after the attack by SpookNet) I learned of this. I was shocked by JustCard's lack of prudence in this regard.

9. Had I 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.

**STATEMENT OF TRUTH**

I believe that the facts stated in this witness statement are true.

Signed: *Philip Frye*

Dated 9 June 2011

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

---

**WITNESS STATEMENT**
**OF MARJORIE HANCOCK**

---

I, Marjorie Hancock, of JustCard Plc, Darwin Industrial Estate, Slough, Berkshire will state as follows:-

1. I am the Chief Executive of JustCard.

2. In late January 2011 JustCard was the victim of a sophisticated cyber attack. I can confirm that we incurred the following costs:

| | |
|---|---|
| Initial fraud losses | £15m |
| Crisis management | £24m |
| Recall of pre-paid cards | £26m |
| Long-term remediation | £5m |
| Other potential liabilities | £3m |

3. JustCard entered into a policy of insurance ("the Policy") with the Defendant with effect from 1 January 2011 to cover just this sort of eventuality. Unfortunately, as it all too often the case, insurers have refused to cover our claim, seeking to dredge up any possible defence to avoid having to pay out. I have been asked to address in this statement the following issues:

   3.1. The upgrade to ProcessSys in autumn 2010 for which JustCard declined to pay;

   3.2. The decision to reinstate and the process of reinstating customers' balances where they had been depleted by XYZ's fraud; and

   3.3. The decision making process which led to the incurring of crisis management costs in the immediate aftermath of the cyber attack.

**The upgrade**

4. In 2008 JustCard entered into a contract with a software design and support company called Software Solutions Ltd. Software Solutions wrote and implemented ProcessSys for JustCard in 2009. The system, which enables us to process payments on our prepaid cards, was designed for us and our requirements, but Software Solutions retained the copyright and the right to sell the software to other companies which were not in direct competition with JustCard.

5. At the beginning of November 2010 a new upgrade for ProcessSys was made available by Software Solutions Limited. However, the cost of the upgrade was over £2 million. JustCard was in some financial difficulty at the time and could not really afford this. Accordingly, we did not purchase the upgrade.

**Reinstating customer balances**

6. In the immediate aftermath of the cyber attack, one of my prime concerns, obviously, was to maintain JustCard's good reputation with its customers and to ensure that none of them was put to any financial loss by reason of this attack, which, after all, was certainly not any of their faults. As I have said, I was told about the attack on 1 February 2011. That afternoon, I instructed our Security and Accounts department to ascertain as quickly as possible which payments had been made by reason of the fraud. This was not particularly difficult to do, because generally the payments had been made from ATMs geographically very distant from the relevant customer's address. By about 9:00 am on 2 February 2011, they had what they thought was a reasonably complete list of the affected customers. I immediately authorised that each of those balances should be re-credited with the money that had been wrongly withdrawn, and that was in effect by lunchtime that day.

**Crisis management costs**

7. Ms Avery informed insurers of the attack on 2 February 2011. As the Court will, I expect, understand, the immediate aftermath of the cyber attack was extremely busy. Whilst we recognised the importance of notifying insurers as quickly as possible, my primary concern was to preserve the reputation of JustCard by making sure no customer was inconvenienced and ensuring, as quickly as possible, that no further attacks could be carried out.

**STATEMENT OF TRUTH**

I believe that the facts stated in this witness statement are true.

Signed: *Marjorie Hancock*

Dated 10 June 2011

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 special[5]. 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 warranty[7]. 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 attach 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 test[10]. 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

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

---

**DEFENDANT'S SKELETON ARGUMENT**

---

1 In these proceedings the claimant assured ("JustCard") claims an indemnity under a Cyber Protection Insurance Policy ("the Policy") issued by the defendant insurer ("Cybersafe") in respect of losses suffered and expenses incurred following the "hacking" by Spooknet of JustCard's processing system between 26 and 28 January 2011.

2 Cybersafe denies that it is liable to indemnify JustCard under the Policy in respect of the sums claimed or at all. It sets out the grounds for that denial under the following headings below: (1) JustCard's failure to upgrade its Processing System; (2) JustCard's claim pursuant to Insuring Agreement 3; and (3) JustCard's claim pursuant to Insuring Agreement 6.

3 The parties have agreed and the Court has directed that the present hearing deal only with issues of principle and that matters of detail (including the reasonableness of any particular expense incurred) be dealt with at a later hearing.

**JustCard's failure to upgrade its processing system**

4 JustCard used a bespoke specialist software system designed by Software Solutions Limited called ProcessSys. The version of that system purchased by JustCard was known as edition 3.16. Prior the Policy being placed, an upgrade, known as edition 3.17 and offering improved security, had become available. JustCard, however, chose not to purchase edition 3.17. Cybersafe understand that JustCard took this decision on grounds of cost.

5 The above matters were not disclosed to Cybersafe at placement. Thus, while Cybersafe was provided with details of ProcessSys edition 3.16, it was not told of the existence of edition 3.17 or of JustCard's decision not to purchase that upgrade.

6 If JustCard had purchased 3.17 then this would have prevented the hacking of JustCard's systems the subject of the claim. The hackers used a form of "buffer overflow" known as "Quizling" to access the JustCard system. Edition 3.16 had a flaw which made it vulnerable to such an attack. This flaw was corrected in version 3.17.

7 In the above circumstances, Cybersafe is entitled to avoid for non-disclosure; alternatively JustCard's claim is excluded from cover pursuant to exclusion 2A to the Policy.

*Non-Disclosure*

8 Cybersafe says that the non-disclosure of JustCard's decision not to purchase edition 3.17 was both material and induced it to offer cover on the terms that it did. Cybersafe relies in this respect on the evidence of its underwriter Mr Frye (the parties have agreed that no independent expert underwriting evidence will be called and that Cybersafe can rely on Mr Frye's evidence in relation to the issue of materiality).

9 Contrary to JustCard's contentions, the presentation made to Mr Frye was not fair. It omitted a key fact, namely the availability of edition 3.17 and JustCard's decision not to purchase that upgrade. It is trite law that an underwriter is not required to be a detective (but see, if necessary, the decision in ***WISE***, cited by JustCard, at paragraph 42). He is not required to question the assured to elicit facts which should have been included in the presentation. Instead, it is the duty of the assured to ensure that the disclosure made is full and frank. This did not occur in the present case.

10 It follows that there can be no question of Cybersafe having waived disclosure as a result of Mr Frye not enquiring as to whether there were any upgrades available. Mr Frye was entitled to assume that that JustCard's software was up to date unless told the contrary. There was nothing in the presentation made to Mr Frye which might have put him on notice that there was an upgrade available which JustCard had chosen not to purchase. The situation is fundamentally different from those cases where a failure to enquire has been held to give rise to a waiver (see, for example, the decision in ***Pan Atlantic*** cited by JustCard where the assured disclosed its claims records for some years but not others and it was held that the underwriters failure to enquire about those other years gave rise to a waiver).

11 Nor does the fact that policy was subject to exclusion 2A (which is set out below and is concerned with claims arising out of a failure to update a system) affect the materiality of JustCard's decision not to purchase edition 3.17 or relieve JustCard of its obligation to disclose that decision. In this respect JustCard seeks to rely on the general rule (which finds statutory basis in section 18(3)(d) of the Marine Insurance Act 1906) that an assured is not obliged to disclose "that which is superfluous to disclose by reason of any express or implied warranty" and contends that a similar approach can be adopted in relation to matters covered by exclusions.

12 This argument is misconceived. The above rule will apply where the existence of a particular state of affairs is warranted. Breach of that warranty will discharge the cover. In the circumstances, disclosure of matters the subject of the warranty is superfluous.

The position is very different in relation to an exclusion. In the case of an exclusion no promise is given as to the existence of a particular state of affairs and there is no remedy of discharge. Instead, the effect of an exclusion is to limit the cover provided by excluding certain types of claim.

13 The distinction between warranties and exclusions is illustrated by the present case. If it had been warranted that best efforts would be used to install all available updates, then there would have been no need for JustCard to disclose its decision not to purchase edition 3.17 (but the cover would have been discharged as a result of JustCard's failure to purchase edition 3.17). In the absence of such a warranty, JustCard's decision not to purchase edition 3.17 was material and needed to be disclosed.

*Exclusion 2A*

14 Exclusion 2A provides as follows:-

> "*We shall not be liable for any claim directly or indirectly arising out of or in any way attributable to:*
>
> *2A. 1. …*
>
> *2. the failure to use best efforts to install commercially available software product updates and releases, to apply security related patches, to computers and other components of the Insured Organization's Computer Systems.*"

15 JustCard contends that the above exclusion does not apply because its decision not to purchase edition 3.17 was reasonable in all the circumstances (that is having regard to the cost of the upgrade and the fact that the ProcessSys was, even without the upgrade, a very modern system). Cybersafe does not accept that JustCard's decision was in fact reasonable, but says that, in any event, this is irrelevant. The exclusion does not allow JustCard a discretion as to whether or not upgrades are to be installed. Instead it imposes a positive obligation upon JustCard to use best efforts to install all commercially available updates. JustCard did not do this. It made no efforts to obtain or install edition 3.17.

16 JustCard also argues that its claim is not a claim "directly or indirectly arising out of or in any way attributable to" its decision not to purchase edition 3.17. This is on the basis that even if edition 3.17 had been installed Spooknet or an associate of Spooknet would still have attacked its systems and would have been able to circumvent (albeit by somewhat different means) the improved security provided by edition 3.17.

17 This argument confuses the loss which has occurred and which is the subject of JustCard's claim (an attack by Spooknet on 26 to 28 January 2011 which successfully circumvented edition 3.16 using the Quizling technique) with a loss which has not occurred and in respect of which no claim is made (a hypothetical attack by Spooknet or an associate on a date unknown which might have circumvented edition 3.17 using a different technique). The actual loss which occurred was caused by JustCard's failure to purchase edition 3.17. That edition would have prevented Spooknet gaining access to JustCard's system using the Quizling technique. It is that loss in respect of which

JustCard seeks to make claim. Accordingly, exclusion 2A applies. It matters not that if JustCard had purchased edition 3.17 it might still have been attacked and suffered loss.

**JustCard's claim pursuant to Insuring Agreement 3**

18 Insuring Agreement 3 provides as follows:-

> "*We shall pay on your behalf all damages and defence costs which exceed your excess as stated within item 4 of the Schedule, which you become legally obliged to pay as a result of any claim first made against you 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, arising from a security breach or privacy breach by you or others on your behalf for whom you are legally responsible…*

19 Cybersafe understands that JustCard seeks an indemnity pursuant to Insuring Agreement 3 in respect of the following sums:-

(1) £15.8 million; this being the total of the sums which were withdrawn by Spooknet and which were then re-credited by JustCard to its customers' accounts.

(2) £26 million; this being the total costs incurred by JustCard in recalling customers' pre-paid cards. Cybersafe understands JustCard to contend that such sums are recoverable as mitigation costs, incurred so as to prevent further withdrawals by Spooknet as referred to in (1) above.

20 The first point to be made is that the withdrawals made by Spooknet constituted a loss to JustCard, not its customers. This is because such withdrawals were unauthorised. Accordingly, JustCard continued to be liable to its customers in respect of the pre-existing balances on their cards and the money paid out was money belonging to JustCard, not its customers. In the circumstances there can be no question of JustCard being entitled to recover under Insuring Agreement 3 in respect of such withdrawals or its re-crediting of customers' account. Insuring Agreement 3 does not provide cover for losses suffered by JustCard itself. JustCard's re-crediting of customer accounts simply reflected what was the correct legal position (that is that the debits previously made were unauthorised and of no effect).

21 Further, no customer has made any claim against JustCard and JustCard has not at any relevant time been legally obliged to pay damages to any customer in respect of a claim made by it as required by Insuring Agreement 3. JustCard seek to answer this objection by saying that if it had not re-credited customers' accounts, they would have made claims against it. This may be right but is nothing to the point. The cover provided is in respect of a legal liability for damages in respect of a claim. It does not include costs incurred to avoid such a claim being made. The Policy does not contain any "mitigation clause" (i.e. a clause providing cover for costs incurred in mitigating an insured loss).

22 Further, if JustCard had refused to re-credit customers' accounts and customers had then made claim against it, any award of damages in favour of the customer would not be recoverable under Insuring Agreement 3. This is because such liability would not arise out of an insured wrongful act (such as a cyber attack) but instead arise out of a refusal by JustCard to pay to customers sums to which they were contractually entitled.

23 So far as the £26 million of recall costs is concerned, JustCard argues these are recoverable as mitigation costs. However (and as stated above) the Policy contains no mitigation clause and does not provide cover for mitigation costs. Further, the loss which JustCard claims it was seeking to mitigate (further withdrawals by Spooknet leading to further re-crediting of customer accounts) was not an insured loss. Accordingly even if mitigation costs were otherwise recoverable under the Policy, these costs would not be because they were not incurred in mitigating an insured loss.

**JustCard's claim pursuant to Insuring Agreement 6**

24 JustCard seeks to recover £24 million pursuant to Insuring Agreement 6 in respect of "Crisis Management Costs". That term is defined in the Policy as follows-

> "*Crisis management costs means any fees reasonably incurred by you and approved by us for the employment of a public relations consultant if you reasonably consider that action is needed in order to avert or mitigate any material damage to any of your brands and which constitutes a newsworthy event that has been notified to us and has arisen due to a claim.*"

25 The effect of the above definition is that costs can only be Crisis Management Costs and will only be recoverable as such under the Policy if they have been approved by Cybersafe. It is accepted that in the present case JustCard did not at any time seek or obtain Cybersafe's approval in respect of the costs of £24 million referred to above. As a result such costs are irrecoverable under the Policy.

26 JustCard says that its failure to seek and obtain Cybersafe's approval was unintentional and asserts that what it did by way of crisis management was exemplary. Even if true, this is irrelevant. The Policy only covers costs approved by Cybersafe.

27 JustCard argues that the above definition does not require Cybersafe's approval to have been obtained before the relevant costs were occurred. While it is accepted that the definition does not use the phrase "prior approval" (or some equivalent) it is nonetheless clear from the use of the past tense ("*approved by you*") that the approval referred to is approval given before the costs have been incurred. In this respect it will be appreciated that if approval could be sought and given after the event, then difficult questions would arise as to what factors Cybersafe could take into account when deciding whether to give its approval and, in particular, as to what regard it could have to events occurring after the costs were incurred.

28 JustCard also argues that the Policy is subject to an implied term that Cybersafe cannot withhold its approval unreasonably. There is no basis for any such implication. The position is analogous to that considered by the Court of Appeal in ***Gan Insurance Co Ltd v Tai Ping Insurance Co Ltd (Nos 2 and 3)*** [2001] Lloyd's LR (I & R) 667. Just as in that case it was held that a requirement that a reinsurer's consent be obtained to any settlement was not subject to an implied term that that consent not be unreasonably withheld, so in the present case there is no requirement that Cybersafe should not unreasonably withhold its approval of Crisis Management Costs.

29 The above issue arises only in the event that the Court holds (contrary to the above) that JustCard is entitled now to seek Cybersafe of the costs it has incurred in respect of crisis management. In such circumstances Cybersafe asks the Court to direct that its right to give or withhold approval is unfettered save that (as set out in ***Tai Ping***) it must act in

good faith and only have regard to relevant considerations and not reach a decision which is “Wednesbury” unreasonable (i.e. so unreasonable that no insurer in its position could reasonably reach such a decision).

**TOM WEITZMAN QC**

**NICHOLAS CRAIG**

**3 Verulam Buildings**