

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