

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 TODD ROLLAND**

I, Todd Rolland, of Rolland Dean, 12 High Street, Bromley, will state as follows:-

1. I am a forensic investigator and director of Rolland Dean. Rolland Dean was established in 2005 by Mr Dean and me to offer specialist advice in relation to cyber attacks of all kinds. Mr Dean and I are well known in the industry and both of us regularly give presentations and write papers in relation to current cyber risks.
2. On 1 February 2011, Ms Avery of JustCard rang me to seek our assistance in relation to a serious cyber attack suffered by JustCard. Rolland Dean was able to promptly and efficiently provide our services to JustCard.
3. I have been asked in this witness statement to give a brief description of how the attack happened, and to explain to the Court the consequences of Software Solutions Ltd having failed properly to upgrade the software in Autumn 2010.
4. The attack was made by SpookNet, who are a notorious cyber attack group. Their whereabouts and identity are not known, but they have been responsible for several brazen and well publicised attacks on financial institutions.
5. This particular case was a classic SpookNet attack, in that they used a technique known as "Quizling". This involves accessing a system by using a variant of the so-called "buffer overflow" technique. While the details of this type of attack are complex, I am able to explain the basic principles of buffer overflow attacks relatively simply:
 - 5.1. Whenever software receives data for processing, it must ask the operating system to allocate it a sufficiently large chunk of memory, known as a "buffer", into which the data can be loaded for processing. It is the responsibility of the software receiving the data to ensure that it requests a buffer of sufficient size to store the data it is expecting. If the data that arrives does not fit in the buffer (either because the software failed to request a buffer of sufficient size or because the computer has insufficient memory available)

it is the responsibility of software to truncate the data so that it fits into the available space or to reject the data altogether.

- 5.2. If, owing to a bug or design flaw, software does not truncate or reject incoming data that is too large to fit in the allocated buffer, the data is written to a chunk of memory that has not been allocated to that purpose and may well be being used for something else, such as to store the queue of instructions that the processor is about to execute (known as "the Instruction Stack"). This is called a "buffer overflow". When buffer overflows occur, the typical result is that the software (or even the whole computer) crashes.
- 5.3. A buffer overflow attack involves exploiting a design flaw of the type explained above by deliberately sending more data to software than the software is expecting to receive so that the allocated memory buffer overflows. The data sent (known as the "payload") is cleverly crafted so that rather than resulting in a software crash, it results in changes to the Instruction Queue that change the behavior of the software so as to allow the attacker to take over control of the computer and access, for example, the customer accounts.
6. ProcessSys is a bespoke system written by Software Solutions Ltd for JustCard. It was written in a reasonably competent way and took account of the relevant security guidance at that time: including, in particular, the guidance set out in Security Guidance edition 3.16. The guidance included a specific technique for protecting against buffer overflow attacks, which involved using special memory management routines designed to ensure that software cannot write to memory that the operating system has not allocated to it. ProcessSys incorporated those routines properly in accordance with the Guidance. Unfortunately, however, SpookNet found a flaw in the buffer overflow protection routines which they were able to exploit to circumvent the protection.
7. In about November 2010, edition 3.17 of the Security Guidance was issued. This addressed some new forms of cyber attack which had been developed, including the technique used by SpookNet to circumvent the buffer overflow protection in ProcessSys. Version 3.17 contained some technical guidance which would have prevented SpookNet from entering and gaining control of the ProcessSys software in the way they did.
8. However, I am in no doubt that had ProcessSys been upgraded in line with version 3.17, SpookNet would not have been prevented from carrying out the cyber attack because SpookNet, or a group closely affiliated with them, carried out a very similar attack in March 2011 on a Brazilian bank which had systems which were compliant with version 3.17. I should not say too much more about that attack, because it is confidential. Suffice it to say that it is relatively well known within the industry that Version 3.17 was not a material improvement on Version 3.16.

STATEMENT OF TRUTH

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

Signed: *Todd Rolland*

Dated 10 June 2011