

## Afterthoughts on the Castleton case

### 1. Approach to SSC staff

In the summer of 2006 I was asked directly by the Security Manager whether I would be prepared to speak to a solicitor about a call I had dealt with in February 2004. My initial response was that this was not the normal process, but he reassured me that it was more or less a formality so somewhat reluctantly I agreed.

Subsequently, before the meeting with the solicitor, he asked me what my availability was in the autumn for the court case. This was the first time there was any mention of the possibility of having to go to court. Repeated assurances that this would all be settled before getting to court proved to be unfounded.

I appreciate that there may be circumstances where witnesses are summoned and have no option but to comply, but I was not at all happy about how this was handled.

### 2. Review of technical evidence

When I took the initial call in February 2004, I spent only a few hours on it before deciding that I could not see any sign of a system problem. I looked only at a couple of week's information.

While in this case I am now sure that I did not miss anything, and my initial analysis was correct, I am concerned that there was no technical review of the Horizon evidence between the original call and the case going to court. It is probable that any system problem affecting the accounts would have shown up to Post Office staff who did check all the figures very carefully, but since the postmaster was blaming the system for the losses I think it would have been sensible to have double checked this within Fujitsu before it got as far as court. I was certainly concerned, in the early stages, that there might be something I had missed.

Once in court, I found myself being treated as an **expert** witness and answering a wide variety of questions about the system, although nominally I was a **witness of fact** and my witness statement covered just the investigation done in 2004. Fortunately I do have extensive knowledge of the system and was able to fulfil the wider role – but what would have happened if the initial call had been handled by a less experienced SSC person?

If there is a similar case in the future, where the system is being blamed, would it not be sensible to have a technical review of all the evidence, at the first indication that a case may be going to court? Someone involved in that review would then be well placed to give evidence in court.

### 3. Disclosure of evidence

Fujitsu made a major legal blunder by not disclosing all the relevant evidence that was in existence. I found myself in the invidious position of being aware that some information (Tivoli event logs) existed, but not sure whether they had been disclosed or not, since I had not been party to any of the requests for disclosure. It became evident in court that they had not been disclosed.

Quoting from an e-mail received from POL's solicitor after my revelation:

"In any litigation, the parties involved have a continuing obligation pursuant to the Court rules to disclose all documents that may help or hinder their case or the other side's case. In this context, a "document" means anything in which information of any description is recorded, so it includes, just for example, a computer database. Previously, I had asked Fujitsu to let me have all the info it had and had been helpfully given HSH call logs, transaction logs and events logs. I was also recently told that there was a message store which had everything else on it and we invited Mr Castleton to look at it this, but he didn't take up the opportunity."

This suggests that disclosure of the message store itself was an afterthought, though it is fundamental to the system. I know that for fraud cases the 'transaction log' and 'event log' are extracted from the full messages store and submitted, but surely the full message store has to be disclosed in all cases?

Many other files are also archived to the audit servers as a matter of course and could hold relevant information, although the Security team are not necessarily aware of their existence or potential relevance. I'd like to suggest that a list of these files is compiled so that similar mistakes are not made in future.

And what about calls on Peak, which may have evidence attached? And any evidence which might have been kept within SSC? I was not asked whether I had anything that might have been relevant (as it happens, in this case I did not).

Of course there may be subtleties to this that I am unaware of, whereby data may exist but there is no obligation to disclose it. If this is the case, could any future witnesses be briefed appropriately? The response 'no-one has ever asked for that before' does not seem to be a good reason for non-disclosure.

#### **4. Helpdesk calls**

This case highlighted a common problem, both in 2004 and now. The postmaster raised many calls about his continuing losses, both with Horizon and with the NBSC. These kept being bounced and it took weeks before a call was passed to SSC.

Strictly speaking, problems with discrepancies do need to be investigated by NBSC in the first instance, but where there are continuing unresolved problems it should be possible to get the issue investigated properly, and one of the helpdesks should be prepared to take responsibility for the incident. Personally I think the fact that the Horizon helpdesk is penalised for passing 'Advice and Guidance' type calls on to third line leads to too many calls being closed without proper investigation or resolution. This is very frustrating for postmasters, though possibly not an issue of concern to POL.

Anne Chambers  
29/1/2007