POL00000689

Filed on behalf of the: Defendant
Witness: S.P. Parker
Statement No: Third
Date Made: 28 February 2019
Claim No: HQ16X01238, HQ17X02637 & HQ17X04248

THE POST OFFICE GROUP LITIGATION
IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ROYAL COURTS OF JUSTICE
B E T W E E N:

ALAN BATES & OTHERS

Claimant

AND

POST OFFICE LIMITED

Defendant

THIRD WITNESS STATEMENT OF STEPHEN PAUL PARKER

I, STEPHEN PAUL PARKER of Lovelace Road, Bracknell, Berkshire RG12 8SN WILL SAY as follows:

1. This is my third witness statement in relation to these proceedings. The facts set out in this statement are within my own knowledge, or if they are outside my knowledge, I have explained the source of my information or belief.

2. I have been asked to comment on two new issues that have been raised in Mr Coyne's Supplemental Report (**Coyne 2**), to address a point made by Mr Coyne in relation to "remote access" and to address two short points arising from my first two witness statements.

HOW SSC IDENTIFIES BRANCHES AFFECTED BY A BUG

3. At a number of points in Coyne 2, Mr Coyne comments that he has not seen evidence of effects of a bug which had financial impact on a branch being remedied. It is part of the SSC's standard diagnostic process that, when we have identified a bug, we also seek to identify all areas of the system affected by that bug. Where the bug has caused discrepancies in branch accounts so as to create an incorrect shortfall or surplus, we take steps to identify all branches that

POL00000689

have been impacted. This is our standard practice and to the best of my knowledge it has always been done since Horizon was first introduced.

4. The way in which this is done depends upon the nature of the issue. A bug invariably gives rise a repeating pattern or trail in the data held in Horizon or on other related systems. Some bugs give rise to effects that would be picked up by reports within Horizon and corrected as a matter of routine by Fujitsu and / or Post Office. A bug causing a payments and receipts mismatch giving rise to a BIMS would be a good example of this (see further below). For others, identifying branches affected by a bug is usually done by identifying that unique or near unique pattern and then looking for incidents of it in relation to other branches.

5. Where a bug has affected branch accounts it is not usually difficult to identify the affected branches and the impact on their accounts. Since Horizon Online was introduced, the SSC has used methods such as:-

   5.1 manually building and executing a SQL search of transaction data held in the Branch Support Database;

   5.2 searching counter and system event information held in the Event Reporting Platform (commonly referred to as the ERP);

   5.3 searching for markers or identifying patterns in other data; and

   5.4 setting up bespoke reporting that looks for the symptoms caused by the bug.

6. Similar methods were used in Legacy Horizon (although it should be noted that the main counter transaction store was the Riposte message store rather than what is now the central branch database (**BRDB**)).

7. In terms of documentation, there is no particular template document or report generated to track the output of these results as they may be different in different cases. It should be kept in mind that the number of bugs of this type are a very small fraction of the work undertaken by the SSC so spending time building standard template documents for this would not be proportionate The action taken is sometimes recorded in Peaks although as noted in paragraph 41.3 of my first statement, Peaks are essentially notes made by Fujitsu personnel to chart the progress made in resolving an issue and these notes can vary in fullness and clarity. Peaks focus on solving the underlying root cause of a bug and would not typically be the place to record the subsequent remedial action across the estate. {E2/11/11}

POL00000689

8. Once Fujitsu has identified the branches affected by a bug, the information (or the process for identifying affected branches) is passed to Post Office, usually by Fujitsu's Service Delivery team. This is not my area, but I have a basic understanding of how it works.

9. For minor issues, the information would usually be provided to Post Office by email but for major issues, it might be provided in a Major Incident Report or something similar. For example, SVM/SDM/REP/3187 {POL-0146852} is the Major Incident Report that was prepared following an outage at branches that caused transactions to fail on 9 May 2016. A Post Incident Report was also prepared following this incident "*to identify the underlying causes of the service outages and identify corrective actions and service improvements which shall eliminate repeats and improve the incident management processes*" (SVM/SDM/INR/3140 {POL-0151605}).

10. Information may also be passed to Post Office as part of a routine process like a Business Incident Management Service (**BIMS**) report. As I explained in paragraph 44 of my first statement, there was (and is) a process run by the Management Support Unit (**MSU**) which involves examination of various system reporting and may result in BIMS entries going to Post Office. The following BIMS reports were sent to Post Office in relation to the 9 May 2016 outage referred to above: {POL-0514573}; {POL-0514574}; and {POL-0514575}. {E2/11/12}

11. As I understand it, there are a number of ways in which Post Office may take corrective action and how it chooses to do this will depends on the nature of the issue. One possible way of doing it would be by issuing a Transaction Correction to restore the branch to the correct position.

12. This process of identifying a bug, then identifying it effects and then remedying those effects is not special to Horizon. It is a standard part of any IT support practice.

APPSUP

13. Paragraph 3.277 of Coyne 2 refers to the use of APPSUP by my team. APPSUP is the more technically accurate name for a type of privileged user access to the BRDB. It is not a distinct or new type of "remote access". My colleague Torstein Godeseth discusses the technical features of the APPSUP role in his third statement. I have been asked to comment on its use by my team. {D2/4/82}

14. Mr Coyne has made what appears to me to be an understandable mistake in his analysis of the privileged user logs at paragraph 3.281. He says that those logs suggest that the APPSUP role has been used 2,175 times to make emergency {D2/4/83}

POL00000689

amendments to the BRDB. This appears to assume that APPSUP is only used for emergency amendments – an assumption which appears to be drawn from his reading of Peak PC0208119. However, this is an administrative Peak which concerns one topic (changing the generic role for SSC database users, which affected the running of development delivered scripts). It does not refer to a particular support action on a live branch. {F/768}

15. APPSUP is used by SSC for updates to and maintenance of the BRDB that would not involve changing transaction data. I have not examined the privileged user logs, but based on my experience my expectation is that these uses of APPSUP, or at least the vast majority, are for support work that does not involve changes to transaction data. I cannot recall any cases in which it has been used to change transaction data, but I cannot state unequivocally that there are no circumstances in which it has ever happened.

16. In paragraph 34 of my second statement I explained that the SSC was (and is) hugely reluctant to change transaction data as that was not their job and they recognised the seriousness of doing so and I stand by that statement. {E2/12/11}

INJECTING TRANSACTIONS (LEGACY HORIZON)

17. Post Office's solicitors have drawn to my attention the two examples of data being injected in Legacy Horizon cited at paragraphs 3.224 and 3.232 of Coyne 2 Mr Coyne refers to these being examples of Fujitsu making a modification to the data within the branch accounts. However, the data was not modified; new data was injected with its own identifiable audit trail:- {D2/4/70}; {D2/4/72}

17.1 PC0128969 {POL-0299414} includes an entry from Martin McConnell at 14:14:25 on 22 November 2005 which states that he advised "on a possible fix whereby we reset the Rollover trailer point back to that of the CAP Rollover trailer." This would have been effected by inserting a new Riposte configuration object written to force the balancing to start from the previous Balancing Period and this would have been recorded in the Messagestore and audit; no transaction data would have been changed.

18. The wording of PC0146094 {POL-0316426} implies that messages were added ("*260020 - Opening figures messages added using ripostemessagefile to convert the £9.56 ROL to cash*"). These messages corrected the opening figures at the branch for a particular product (Romanian Lei) and did not affect transaction data.

19. The vast majority of server injections would not have been to inject transaction data. In paragraph 29 of my second witness statement I listed the circumstances in which data was injected into a counter in Legacy Horizon while Richard Roll {E2/12/10}

POL00000689

was employed by Post Office. Of the six circumstances listed, only one involved transaction data being injected.

MY FIRST WITNESS STATEMENT

20. In paragraph 19 of my first witness statement, I stated that it was not possible in Legacy Horizon to edit or delete data that had been committed to the message store. I have been asked to clarify this statement.

21. At paragraph 19 of my first statement I refer to paragraph 37 of my colleague Torstein Godeseth's first statement, where he explains that the Riposte product managed the message store and it did not allow any message to be updated or deleted from the message store. In some circumstances in Legacy Horizon (see for example paragraph 55.4 of my first statement, which describes action that the SSC took when a counter became corrupted) it would be necessary for the SSC to delete the message store file (and hence all the transaction data it held) to allow Riposte to replicate a full and complete copy of that transaction data from another source. This process does not allow any partial deletion: it is an all or nothing operation. It is a similar process to recovering all your data from a backup.

{E2/11/4}; {E2/1}

{E2/11/16}

22. I do not consider the removal of incomplete or corrupted storage files, to allow the facilities of the system to recover from alternative copies, to be the deletion of transaction data.

MY SECOND WITNESS STATEMENT

23. In paragraph 35 of my second witness statement I stated that, in theory, someone could have used a transaction injection in Legacy Horizon to carry out a transaction such as a GIRO bank transfer or a utility bill payment. In a footnote I explained that GIRO bank transactions are automated payment (**AP**) transactions, like utility bill payments, and that other bank transactions go through a different path, as that was my understanding at the time. Having discussed the issue further with colleagues, I now understand that GIRO bank transactions were EPOSS transactions (like all other manual bank transactions) rather than AP transactions. The distinction is that copies of AP transactions are sent to the Post Office client, whereas with EPOSS transactions they are not.

{E2/12/11}

POL00000689

STATEMENT OF TRUTH

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

Signed: GRO

Name: S.P.PARKER

Date: 28/2/19