FUJ00155196

Privileged

Alan Bates & others v Post Office Limited

Coyne 2 Report – Remote Access

Paragraphs 3.221 → 3.287

SUMMARY

- Coyne's Report deals with remote access under 4 headings:
  - Para 3.221 cites numerous Peaks where he says that FJ have been amending branch data.
  - Para 3.249 cites two problems arising from data being re-built, from which Coyne concludes this shows that FJ could rebuild data
  - Para 3.266 deals with Peaks that show FJ deleting data from Horizon.
  - Para 3.277 cites a number of further Peaks that Coyne says show that FJ have been amending branch data.
- It is difficult to understand the structure to and distinction between these sections. They appear inter-related and there are examples in some sections that are the same as in other sections.
- Also each section, has various sub-issues that are not clearly distinguished by Coyne even though they are completely different. The table below shows a full breakdown of the issues raised across all four sections.
- Coyne moves between Horizon and Horizon Online without informing the reader, which is confusing because the remote access to these systems is very different.
- The forms of "remote access" raised by Coyne only relate to the methods of remote access already covered in PO's evidence. There is nothing new.
- PO's statement that there has only been one BT is still correct – Coyne has found no evidence of any further BTs
  - But Coyne seems to be using BT to mean something more than the Transaction Correction Tool in Horizon Online.
- Coyne does not distinguish between changes made to transaction data and changes made to other parts of the system that do not affect transaction data. This gives a misleading impression that lots of changes were made to transaction data.

The commentary below is focused on the data modification issues. Several of these arise from underlying bugs. We have not been able to conduct a full analysis on these underlying bugs, nor are these the focus of Coyne in this part of his report.

FUJ00155196

Privileged

Heading in Coyne 2	Sub issue by para ref in Coyne 2 [Hyperlinks below]	Old Horizon / Horizon Online?	Peak shows change made to transaction data?	Method of "remote access"				
				Inject transaction into correspondence server Old Horizon Godeseth 1 @ 58.10 Parker 2 @ 27	**Rebuild counter data from mirror copy of data** Old Horizon Parker 1 @ 55.3 & Parker 2 @ 36	**Balancing Transaction** Horizon Online Godeseth 1 @ 58	**Privileged user access** Both Horizons Godeseth 1 @ 59	**TIP Repair Tool** Both Horizons Godeseth 1 @ 60
				Post Office headline position on method of remote access?				
				Yes but only one example found of transaction data being changed – Parker 2 @ 27	Yes but only to replicate a mirror copy of the same data. Substantive content of data not changed.	Yes but only happened once	Theoretically possible but no evidence that it has been used to change transaction data	Does not change transaction data
Remote access and branch data alteration – 3.221	3.221 → 3.222	Old Horizon	Yes		X			
	3.223	Horizon Online	No			X		
	3.224 → 3.231	Old Horizon	No	X				
	3.232 → 3.233	Old Horizon	Yes	X				
	3.234 → 3.242	Old Horizon	Yes	X				X
	3.243 → 3.246	Old Horizon	No					X

FUJ00155196

	3.247 → 3.248	Old Horizon	No					X
Data rebuilding – 3.249	3.249 → 3.262	Old Horizon	Yes		X			
	3.263 → 3.265	Old Horizon	Yes		X			
Deletion of data – 3.266	3.266 → 3.269	Horizon Online	No				X	
	3.270	Horizon Online	No				X	
	3.271 → 3.274	Horizon Online	No				X	
	3.275 → 3.276	Horizon Online	No				X	
Peaks with evidence of remote access – 3.277	3.277: APPSUP	Horizon Online	No				X	
	3.283: Policy Adherence	Horizon Online	This is about the governance around deletions rather a technical method of deletion					

FUJ00155196

RESPONSES TO COYNE COMMENTS ON REMOTE ACCESS

Coyne's conclusions on remote access are largely in section 4 (responding to Parker) and section 5 (responding to Worden). His views however build on the analysis in Section 3. As can be seen by the summaries below, the Section 3 analysis is unsound in many respects, which allows us to attack some of Coyne's conclusions in sections 4 and 5. These are set out below.

Coyne ref	Quote from Coyne	WBD comments
4.9	[Global branches]	Addressed by Godeseth 3
4.79 & 4.80	In Mr Parker's witness statement dated 16 November 2018[1] at paragraph 19 Mr Parker states: *"The suggestion that Fujitsu edited or deleted transaction data is not correct. In Legacy Horizon it was not possible to delete or edit messages that had been committed to the message store."* I have provided excerpts from PEAK records that illustrate edits and deletions of messagestore data within the PEAK analysis (Section 3, 'Evidence of Insertions/Deletions within Branch Accounts (Horizon Issue 10)' above).	• 'Evidence of Insertions/Deletions within Branch Accounts (Horizon Issue 10)' starts at para 3.220 and run to 3.287. • Whether Coyne's statement is accurate depends on what you mean by "edit". We mean edit to mean changing a line of existing data. Coyne may mean this to include (i) injections of data, (ii) BTs and (iii) rebuilding data from mirror copies. • There is no evidence in Coyne's report of FJ deleting or changing transaction data in the sense of changing a single transaction in a basket.
4.81	It should be noted that PEAK PC0051855[2] (and others referenced further within this report from paragraph 3.266 onwards) document activities of deletions in relation to messagestore corruptions and issues. Whilst there is a redundant copy of the messagestore (also known as a mirror) that data could be re-instated from, I consider deletion of messagestore items to be deletions of messages (which held transactional data).	• Peak PC0051855 [F/47] is covered at Coyne para 3.221. This is not about deleting data, but rebuilding corrupted data from mirror backups. See more detailed explanation below. • Coyne @ 3.266 deals with Horizon Online only whereas Parker is talking about old Horizon so Coyne is inaccurate here. Also these sections deal the insertion of a new version of the data object, which include the <Deleted:1> tag and not transaction data.
5.407b	In relation to the Transaction Correction Tool referred to within Issue 10 of this report. I have requested the audit file of its usage, in order to	Coyne is misusing the word "balancing transaction" here. A BT means the use of the Transaction Correction Tool to produce a BT in Horizon

[1] {Witness Statement of Stephen Paul Parker, 16 November 2018}
[2] PEAK PC0051855, 5 August 2000 F/47

FUJ00155196

	support or disprove my opinion that this tool has been used more than once. Note that even if has indeed only been used once, Balancing Transactions could still be conducted by Fujitsu SSC (in Legacy Horizon) and through Privileged User access in (Horizon Online).	Online. Anything else has a different name. Coyne is deliberately trying to call everything a BT so to attack PO. Coyne makes reference to having requested the audit file of the Transaction Correction tool. Disclosure was provided on 22 February 2019 (after Coyne 2) [H/218].
5.408a	Mr Godeseth (and subsequently Dr Worden) state that only one Balancing Transaction has been performed (using the Transaction Correction tool) by Fujitsu. However it is evident that more than one Balancing Transaction has been conducted by Fujitsu. More detail in relation to this is provided under Issue 11 in this report.	Same point as above. Only one BT has ever been used to change transaction data.
5.416 and 5.417	Additionally, (as set out in my first report), it was possible for Fujitsu to perform modifications and deletions as they could run commands on the counter machines in branches accessing and querying the hard disk, which they could do through remote access. Fujitsu also had the capabilities of performing modifications and deletions within the branch's database (latterly the BRDB for Horizon Online). This is expanded further under Issue 11 commencing at page 249.	Too vague to comment on.
5.418	It is agreed that remote access and remote control facilities would be required for Fujitsu support purposes.	Remote control facilities are something very different. This is where a support person can take over the machine as if they are acting like a user logged on locally. There is no evidence to support this and Fujitsu have confirmed that this type of access has never been available.
5.422a	Transactions inserted by Fujitsu NOT obviously visible to the Subpostmaster (i.e. balancing transactions inserted into the MessageStore / BRDB and at other points within Horizon processing systems past the Counter).	Same point as above about the definition on balancing transaction.
5.423	Fundamentally, there are two principles to the above, Fujitsu have the ability to insert transactions to fix errors outside of the Subpostmaster's	This particular example relates to Fujitsu's correction of harvester exceptions involving a missing settlement value, which would have

FUJ00155196

	knowledge and without their permission which may not be visible to the Subpostmaster (see paragraph 3.235), and secondly, Post Office have the ability to electronically insert transactions that are acknowledged and visible to the Subpostmaster, in the form of TCs and TAs.	resulted in a receipts and payments mismatch for the branch if not corrected. This involved two fixes for FJ: 1. Fix the data feed to Post Office using the Tip Repair tool. This was used to identify the incomplete TPS transaction and passed onto POLFS to correct the back-end TPS database and did not have the ability to impact branch accounts. 2. Insert an additional balancing transaction message into the branch messagestore to avoid a R&P mismatch. The additional transaction message was inserted to represent the equal and opposite transaction for USD to balance against the original message. As explained below, this did have the ability to affect branch accounts but the messages included audit information to show they were inserted by the SSC and explain the issue.
5.424	A few examples of Fujitsu editing and deleting records from the Horizon branch database are set out in 21 December 2018 disclosure of MSC records: a. Contained within the MSC Documents provided the lines serialised with the codes 043J0262492, 043J0264220 and 043J0265130 record the steps followed to resolve "The Business Problem: To prevent us having to talk unhappy PMs through the complicated workaround described in KEL acha3347Q[3] we need to remove any declarations belonging to stock units deleted since 15th May". These steps display the command "delete from ops$brdb.brdb_branch_decl" which I believe will delete records from the branch database. The document suggests that this will address errors in the branch database caused by an early Horizon bug. These MSC records are also recorded in the PEAK reference PC0199654[4]. b. Document 043J0265683 records the steps followed to resolve; "Current Business Position: There are duplicate rows coming through from BRDB into BRSS.Exact cause is yet unknown.". These steps display the command "DELETE FROM ops$brdb.brdb_pouch_coll_details" which I believe will delete records	These sections are not quoted in section 3 of Coyne. They are covered in Gareth Jenkins' comments on the full review of Coyne 2.

[3] F/702
[4] F/655

FUJ00155196

	from the branch database. The document displays a question; "Does this change need to be assessed by POL?:" the answer in the document is shown as "No.Involves BRSS only" c. MSC043J0355958 records the "SQL insertion" of "Dummy Transaction Acknowledgement" into the branch database to correct a fault within Horizon that was later fixed. This record suggests that the same process had been completed previously under record MSC043J0348236.	
5.438i	PEAK PC01959625[6] created 12 March 2010 relates to the Transaction Correction tool and states: *"The Transaction Correction tool has now been used in live. The templates for use with this tool need to be updated to correct some details. Gareth* *Seemungal is aware of the corrections needed…* *…The proposed fix would correct and update the BRDB transaction correction tool templates, making it less likely that mistakes will occur when SSC are trying to resolve problems with transactions in BRDB."* This suggests that the modifications and balancing transactions conducted by Fujitsu support staff within the BRDB is not unusual.	This is the same comment as made in para 3.223. See detailed analysis below for why this comment is wrong.
5.348ii	Fujitsu were able to insert balancing transactions outside of utilising the Branch Correction tool referred to above. Balancing transactions were not limited to Horizon Online. The PEAKs detailed in the Horizon Issue 10 PEAKs at Section 3 above indicate which of those that relate to balancing transactions.	This is presumably a reference to para 3.221. Misuse of the words "balancing transaction" to extend this to Old Horizon.

[6] F/594

FUJ00155196

i		
5.442	It is my belief, that in review of the PEAKs documented in Section 3 'Evidence of Insertions/Deletions within Branch Accounts (Horizon Issue 10) of this report, that SSC could not only inject/insert or edit transaction data but delete instances of it (and/or operations relating to it, which are of equal importance) also. *Note: This relates only to Legacy Horizon.*	See Godeseth 3 and Parker 3
5.443	At paragraph 1117 I note that Dr Worden inherits his opinion from the evidence provided by Mr Godeseth that messages from the message store (in Legacy Horizon) could not be updated or deleted. However, in my analysis of the PEAK records at Section 3 ('Evidence of Insertions/Deletions within Branch Accounts (Horizon Issue 10)', I have demonstrated that this is not the case. One example of an update (of which further detail can be found in the aforementioned Section 3) is as follows: PC0130275[9] created 21 December 2005 (further detail provided at 3.230 of this report) states [*QUOTED REMOVED*] A further example of deletion (of which there are more at Section 3) is: PEAK PC0057909[10] dated November 2000 (further detail provided in Section 3 at paragraph 3.249) refers to an issue occurring as a result of a branch's counter base unit replacement, and sets out:[…]	The sections cited by Coyne do not show data being deleted or edited. PC0130275[11] @ Coyne 3.230 – no injection of transaction data. At entry 17 January 2006 [14:53] Gerald Barnes describes the number of steps he has taken to try to reproduce the problem. At entry 20 January 2006 [12:32] he confirmed he "*set up a dual counter system with notes 1 and 31 and imported the supplied message store to a date and time of*" to replicate the issue but this didn't work. PC0057909[12] @ Coyne 3.249 – this is an example where replication had been completed while not fully connected to all neighbouring counters, meaning certain messages on counter 1 were different to those on counters 2 and 3. There is no evidence of any remedial work being carried out by SSC in this Peak. This Peak was cloned to Peak PC0058435 F/74. As per 7/74/5, in this instance the SPM reversed the transactions and then was able to recover "*them again on counter 2*" meaning her "*AP is now correct*". While the SPM was concerned that the Balance snapshot and the cheque value was wrong, Fujitsu confirmed (F/74/5) that the cheque listing is ok and advised the SPM to "*see whether the system will allow her to roll over once cheques have been remmed out, and to contact the NBSC for advice on rolling over*". There is therefore no evidence in either the original or cloned Peaks of any remote access or remedial work by Fujitsu here.

[7] F/641
[9] F/323
[10] F/73
[11] F/323
[12] F/73

FUJ00155196

5.452	Fujitsu has no policy, process, procedure or operational practice that calls for it to use its privileged access to edit or delete transaction data.13 Therefore, if Privileged User access was being used (**which I opine that it was**) there is no clear process for it. This introduces a high element of risk as users were not effectively governed or constrained by any form of compliance for its use.	None of the Peaks cited in Section 3 relate to Privileged Users manually editing or deleting transaction data (other than by mirror back-ups, BTs and injections).
5.455	The entire section under the heading: *Implement fixes in Horizon that had the potential to affect transaction data or data in branch accounts*	This section is about implementing fixes not remote access. To the extent that Coyne is saying that fixes could cause further bugs (ie. regression bugs) – this is true but a second order issue. If Coyne is saying that when using privileged user access to implement fixes, a privileged user could make a mistake – there is no evidence of this anywhere in Coyne 2. It is unclear what fixes Coyne is referring to, but normally when fixes were released this would be done as an automatic Work Package that had been tested, rather than being manually deployed by a privileged user.
5.459	The entire section under the heading: *Rebuild transaction data.*	Coyne cross refs to his section 3 @ 3.249 which is under the heading "Data Rebuilding". This entire section relates to Legacy Horizon. This also refers to the automatic process built into Riposte whereby data would be replicated between counters, and if a counter failed, it could be rebuilt from the mirror copy on the other counter. Coyne gives a misleading impression that FJ are manually re-writing data. They are not. They are just triggering the automatic back-up process.

[13] {Witness Statement of Torstein Olav Godeseth, 27 September 2018}

FUJ00155196

SECTION 1: REMOTE ACCESS AND BRANCH DATA ALTERATION: PARAS 3.221 – 3.248

- This section of Coyne's report references many Peaks that he believes to show Fujitsu modifying data.
- There are 7 distinct groupings of issues. Each one of these groups is dealt with below in a separate section of this summary.
- Coyne does not differentiate between old and new Horizon, but this is critical in relation to remote access because the methods of doing this are radically different.
- Six of the groups of issues relate to Old Horizon. All of these are uses of tools that were described in Godeseth and Parker.
- Only one refers to Horizon Online and this appears to be linked to the one known use of a balancing transaction as described in Godeseth.

3.221 → 3.222: Replication of Girobank data from mirror copy

Summary

- Old Horizon.
- Peak documents an instance where the messagestore was deleted and replicated from a mirror copy in Legacy Horizon. This is the same process described at para 55.4 of Parker 1 and paras 36 – 38 of Parker 2

What happened?

- 04.08:2000: the SPM contacted the helpline as their branch giro deposit report was incorrectly showing as 0;
- 04.08.2000: The SPM was first advised to reboot the counter, however, when this did not resolve the issue the helpline advised the SPM to call NBSC the next morning;
- 05.08.2000: Peak opened;
- 05.08.2000: Following investigations into the issue (documented in the Peak) and multiple attempts to reboot the counter, the giro deposit report was still showing as 0. Fujitsu then found that the latest messages from the branch were in the riposte mirror, which meant that they were able to delete the message store and replicate it from the mirror;
- 05:08:2000: the SPM confirmed all data appeared on the relevant report successfully and the Peak was closed.

Impact on branch accounts

- Coyne does not comment on this Peak having any impact on branch accounts.
- Fujitsu note that had the SPM not spotted the zero balance on the report, then this might have caused a financial impact:
    - First, it is unlikely that the SPM would have missed the zero report as that is so unusual. If they did, and proceeded to try to rollover the branch with a zero for Girobank, that might have introduced an error in to the accounts.
    - However, Fujitsu think that this would have likely caused more errors during the process so the branch roll over would have probably failed. This is however speculation because it never happened.

Analysis

- Coyne correctly identifies Peak PC0051855 [F/47] as relating to an incident where the "*messagestore had to be deleted and re-instated from a mirror copy*";

FUJ00155196

- Coyne provides no further analysis, however, appears to be indicating that this shouldn't have happened and that there is some sort of arbitrary process in place that enables Fujitsu to delete transaction data.
- Fujitsu have confirmed this represents an instance where incomplete/ corrupted storage files are being removed, to allow the built in facilities of the system to recover the data from an alternative copy. This is evidenced at various points in the Peak, including:
    - Entry 5 August 2000 [09:28] F/47/1
      "*We will need to destroy the message store and allow it to replicate from the mirror*"
    - Entry 5 August 2000 [10:16] F/47/1
      "*I was convinced that the latest messages from site had not been replicated to the correspondence server, but I have found that they are in the riposte mirror, therefore we can continue to delete the main riposte messagestore*"
    - Entry 5 August 2000 [10:48] F/47/1
      "*The messagestore has completed replicating from the mirror, all the messages are present*."
- Dr Worden's view is that this was an instance where all the branch's transactions were being replicated from one place to another and as such when doing so Fujitsu had no cause to insert or modify transaction data.
- Fujitsu have also confirmed that, during this type of recovery, replication riposte remains offline in recovery mode and as such does not allow any access to the data until recovery/replication is complete with all connected neighbours. This therefore means that Fujitsu had no ability here to insert or modify transaction data.

Relevant Documents

- Peak: PC0051855 [F/47]

FUJ00155196

3.223: Balancing Transaction

Summary

- Horizon Online.
- The Peak[14] referenced by Coyne documents a change to the Transaction Correction Tool that produces BTs. This tool has already been disclosed as described in Godeseth 1.
- It does not refer to a new use of BT – it appears to be a reference to the one and only BT that is known about. Coyne seems to have missed this point.

What happened?

- 12.03.2010: Peak raised to process a change to the Transaction Correction tool, the change being to add a new condition to the tool template;
- 12.03.2010: Confirmation that the change may not be visible to the end user but the "*SSC will be able to fix BRDB transactions quicker and with more confidence*";
- 11.10.2010: Fix delivered through baseline;
- 19.11.2010: Live Support Testing completed;
- 13.01.2011: Fix applied to live.

Impact on branch accounts

- No direct impact on branches. This Peak is just documenting additional ways the tool could be used. It does not relate to a live incident in Horizon.

Analysis

- Coyne says that the Peak suggests that "*modifications by Fujitsu support staff to the Horizon branch database is not unusual*". There is nothing in the Peak to support this.
- Moreover, the Peak says that it has been raised because "*The Transaction Correction tool has now been used in live.*"
    - This entry is made on 12 March 2010.
    - This is 2 days after the one and only BT was used to change transaction data – see Godeseth at para 58.9.
    - Although not stated expressly in the Peak, it would appear that this Peak was raised as a result of this BT – the timing would be massively coincidental if not – and it can be inferred that this was the first time.
    - The Peak therefore shows FJ learning from that one experience
- Coyne selectively quotes from the Peak and in particular quotes that the changes to the tool are "*making it less likely that mistakes will occur when the SSC are trying to resolve problems*".
    - This could be read as if there have been past mistakes.
    - However the Peak also states that:

```
Is this a high-risk area in which changes have
caused problems in the past?
No problems occurred yet - changes to avoid any
potential problems.
```

- Dr Worden's view (from his notes) is that this appears to be an early use of the tool and as such it is likely/ not unusual that there may be small issues to resolve with the tool.

Relevant Documents

- Peak: PC0195962
- First Witness Statement of Torstein Godeseth at para 58.

[14] F/594

FUJ00155196

3.224 → 3.231: Injected object to fix data tree bug

Summary

- Old Horizon
- Injections were made into the message stores but transaction data was not injected.
- This was the injection of a latest (new) version of a Riposte configuration object.
    - Briefly referred to in Parker second statement (29.3, 29.4) but not explicitly documented.
    - Configuration object are used for varied reasons within the Horizon system:
        - Balance Period Configuration
        - Stock Unit Configuration
        - End Of Day Marker
        - User Session
    - Configuration objects are versioned, the latest version being the effective one. By writing a new version of the configuration object the support team can influence the behaviour of the system.
    - In the Peaks below, the configuration object changed was to the balance period. This moved the branch back one balancing period and allowed the SPM to repeat the balancing process with correct data.
    - No transaction data is changed.
    - These configuration messages cannot be seen directly by the SPM, they can only "see" the effect they have (ie. the change in the balancing period). Configuration messages are visible to SSC and anyone who examines the audit trail.

What happened?

Peak PC0128969 [F/312]

- 17.11.2005: Peak PC0128969 raised to deal with a problem experienced by one branch where the SPM's accounts were showing a zero balance on all stock within one stock unit.
- 22.11.2005: Fix suggested which was to reset the stock unit back to previous trading period to enable the SPM to rollover again with the correct figures.
    - Note: FJ think the root cause of this problem is related to the Data Tree issues @ Coyne 3.110. See our separate report on that issue that explains why rolling over again corrects the Data Tree problem.
- 22.11.2005: OCP 12388 [F/312.2] raised
- 24.11.2005: As documented in the OCP 12388 [F/312.2], the stock unit was reset at 15:00 on 24.11.2005
- 28.11.2005: Confirmation in the Peak that the SPM had been phoned to explain process taken to fix the issue.
- 01.12.2005: SPM successfully rolled over. The Stock Unit Balance Report showed a discrepancy in favour of the SPM of £20,737.02 and a corresponding discrepancy in favour of Post Office for the same amount. Confirmation provided in the Peak that these have now cancelled each other out so no loss in the branch.

Impact on branch accounts

- Fujitsu were not altering transaction data (as explained above).
- The underlying bug (with the Data Tree) might have caused a loss. But the fix by FJ was to inject a new data object that moved the stock unit back one balancing period. This did not change any transaction data and would not have caused any discrepancy.

FUJ00155196

- The risk of FJ not rolling the stock unit back is explained in OCP 12388 [F/312.2] at the 'Business risks' section on page 1, which confirms "*If this action is not taken, the Branch Trading Statement due on 30/11/05 will contain incorrect figures*". FJ's actions therefore avoided the branch trading statement having errors in it.

Analysis

- Coyne correctly identifies Peak PC0128969 as representing an instance where the issue of stock unit rollovers returning zero values occurred. He does not seem to have connected this to para 3.110 of his report.
- **Coyne (3.225)** ← the extract quoted shows that it was typical practice for Fujitsu to consult with the SPM where changes of this sort were made so that the SPM understood what is happening and how the issue would be resolved;
- **Coyne (3.231)** states that a solution was to "*amend the stock unit / messagestore data*" and notes that this "*illustrates that Fujitsu can and did alter branch data with any consequent errors not being visible to Post Office or the Subpostmasters unless they were identified and notified by Fujitsu*". The data was not amended/ altered here. Instead, a new Riposte configuration object was written to force the balancing to start from a previous Balancing Period. This was recorded in the message store and audit store in the same way as any other message would be.

What happened?

Background: Branch FAD 147136 and zero value issue

- FAD 147136 is a 5-counter site with 7 stock units.
- On 14 December 2005 the SPM started the process of rolling over stock unit BB. The SPM got to the stage of previewing the Trial Balance, made adjustments and then left the unit logged in until the next day.
- On the following day, 15 December 2005, the SPM previewed the Trial Balance again but it contained only zero values.
- The SPM then rolled over the stock unit from TP8 to TP9 regardless of:
    - the zero values in the Trial Balance
    - the zero values for stock unit BB shown in the Branch Trading Statement

  As a result of the above, stock unit BB was rolled over in an effectively empty state[15].
- The SPM then declared the amount of cash and adjusted the stock levels up to the correct volumes, resulting in a gain of approximately £18,000.

Peak PC0130275 [F/323]

This Peak has been cited by Green a lot in Court and involves branch FAD 147136

- 21.12.2005: Peak PC0130275 raised in response to a call raised by the SPM concerning the stock unit balance report which contains all zeros
- 22.12.2005: Confirmation that Fujitsu is unable to correct the system figures safely[16] but that one solution is to provide the accurate figures for what should have been in the Final Balance for BB from TP8, to allow Post Office to correct the position by way of a Transaction Correction, as suggested by Fujitsu[17].
- 22.12.2005: Investigations confirm that this has occurred previously and been investigated under PC0128969 [F/312][18] but that development were unable to reproduce the problem.
- 03.01.2006: Investigations confirm that the issue has occurred again under PC0130461 [F/324] (also referenced by Coyne at para 3.228)
- 03.01.2006: Call raised to an 'A' priority as 3 instances of the issue have been recorded.

[15] 'Empty state' means no values were transferred from the previous period.
[16] By 'safely', Fujitsu have confirmed that this is subject to interpretation but their reading here is that this means that there would have been no known workaround, meaning any changes attempted would be for the first time and high risk.
[17] Note, Fujitsu do not know how Post Office decided to correct the position.
[18] This is the Peak referenced by Coyne in para 3.224

FUJ00155196

- 12.01.2006: Confirmation that stock unit BB has now successfully rolled over into TP10.
- 12.01.2006: Fujitsu manage to replicate the issue
- 17.01.2006 – 09.02.2006: Fujitsu continue to try to replicate the problem. This is documented in a number of entries, which briefly summarise the steps taken.
- 10.02.2006: potential root cause identified
- 10.02.2006: course of diagnostic action identified to confirm root cause. At this point the root cause has not been identified and Fujitsu are speculating as to what the root cause may be. Fujitsu also confirm here their intention to add in extra diagnostic logging so that if the issue happens again there will be more evidence to examine in future to assist in determining the root cause.
- 23.02.2006: Release Peak PC0132674 raised and subsequently withdrawn
- 07.03.2006: Release Peak PC0133131[19] raised
- 22.03.2006: Testing in LST – here the release containing the new diagnostic code is being tested
- 23.03.2006: KEL CCard525M updated[20]
- 15.05.2006: A further occurrence of the problem recorded under PC0135486[21]
- 25.05.2006: Proposed solution from development. The extra evidence collected from the new occurrence (PC0135486) allowed development to undertake a further investigation and reach conclusions on the root cause, meaning a potential solution was possible.
- 18.08.2006: LST testing completed
- 31.08.2006: Fix released and KEL CCard525M updated

Impact on branch accounts

- The issue did affect branch accounts, however, the fix implemented in 31.08.2006 resolved the issue.

Analysis

- This is a good example where Fujitsu were unable to determine the root cause at the initial stages of the investigation due to lack of evidence, however, implemented additional diagnostic logging so that, if the issue did happen again, they would have more data available to determine the root cause.
- Peak PC0130275 states "*making manual changes to the messagestore is open to error*"
    - FJ comment: *Yes, a support unit would always avoid manual intervention in any part of a system unless necessary, it is open to human error. There is no explicit process here. Any competent support technician would understand the possible implications of manual actions and treat them with appropriate caution. Where we identify a repeatable process to resolve an issue a KEL is raised.*

Relevant Documents

- Peaks: PC0128969[22], PC0130275[23], PC0130461[24], PC0130855[25], OCP referred to in PC0130855: OCP 12630[26],PC0135486[27], PC0137766[28] and PC0137051[29]

[19] Not in trial bundle: POL-0303531
[20] Not in trial bundle: POL-0448152
[21] F/343
[22] F/312
[23] F/323
[24] F/324
[25] F/325
[26] POL-0496675
[27] F/343
[28] F/348
[29] F/346

FUJ00155196

- FJ notes that some of the detail for the above sits in the relevant OCPs: OCP 12578[30], OCP 13795[31], OCP 13964[32] and OCP 12388[33] for the change – these have been disclosed but are not in the bundle:
    - OCP 12578 records the following: update the StockUnit and StockUnitMarker objects for AA, removing references to BP2, BP3 and BP4. The BPMarker objects themselves will be deprecated by a new version.

[30] POL-0496629
[31] POL-0497843
[32] POL-0498001
[33] F/312.2

FUJ00155196

3.232 → 3.233: Injection of Romanian Lei transaction data

- Old Horizon
- This is a form of message injection as described in Torstein 1.
- This does not involve a transaction being injected, but the injection did change the accounts.

What happened?

- Coyne references two Peaks[34] that relate to an issue caused by the removal of reference data.
- See our note on Coyne 3.132 for general background information on Post Office withdrawing products from branch but this is not the same underlying issue. There does not appear to have been any bug in the current case.
- Post Office withdrew the sale of Romanian Lei currency. The SPM was required to rem out the remaining currency to Post Office. They did it incorrectly and left 1p worth of currency in the branch accounts.[35]
- When the branch came to balance, they had a 1p discrepancy for Romanian Lei (because they did not physically have this stock in branch). Ordinarily, the branch would do a stock adjustment (foreign currency is classed as stock in branches, not cash. Cash only ever means Sterling). This would reduce the Romanian Lei by 1p and increase the cash holdings by 1p.
- However, by this time, PO had withdrawn the reference data for the Romanian Lei from Horizon, which meant there was no way on Horizon to adjust the stock. The option do so no longer existed on the screen.
- This left the branch stuck with 1p of Romanian Lei which was preventing them from rolling over (because all stock discrepancies must be resolved before Horizon will allow a rollover).
- The issue was fixed by FJ injecting transactions for the stock adjustment. FJ effectively used it remote access capability to do the stock adjustment that the branch could not do for themselves.
    - It did this by injecting two transaction.
        - One injection add 1p of Romanian Lei thereby offsetting the -1p discrepancy and bringing the accounts to zero.
        - The second was to deduct 1p from cash, creating a -1p discrepancy to balance out the above.
    - The SPM could then make good or settle centrally the 1p cash shortfall. This is the standard procedure where there is a discrepancy. Here, as the SPM should have remmed out the product, when Fujitsu transferred it to cash, this created the 1p discrepancy. We have not spoken to Post Office to see if how this particular discrepancy was resolved but let us know if you would like us to do so.

Dates

- 15.05.2007: Peak PC0146066[36] opened as a result of SPM raising a query with NBSC regarding a cash discrepancy of -1p in foreign currency, which meant the branch was unable to rollover.
- 16.05.2007: Issue investigated and confirmation that the balance snapshot shows the foreign currency sterling value is -0.01. Root cause of -1p then identified as a result of an opening figure of -1pm worth of Romanian currency and that reference data had been removed.
- 18.05.2007: Messages injected to correct the issue.

Impact on branch accounts

- The accounting record was changed but no overall financial impact for the branch.

Analysis

[34] PC0146066 [F/416] and PC0146094 [F/417]
[35] This is not documented in the Peak as such, but if the SPM had properly remmed out the remaining currency to Post Office, there would have been a zero figure.
[36] F/416

FUJ00155196

- Coyne **(3.233)** says that "*It appears that this was likely a modification to the data within the branch accounts*". This is arguably correct.
- All changes, as explained in the Peak, were documented by comments that would have been "*added to the messages to make it clear these had been put in by the SSC*".

    - FJ comment: "*On the rare occasions we had to enter new transactions (as opposed to Objects) we added Riposte Attribute Grammar tags to identify that it was added by the SSC (and also set the Node Id to 99 which was a value not used elsewhere in the system. The Node ID would be visible to the PM on transactions reports but the SSC Data tag would only appear in Audit. Note that it was possible to do this type of work without these measures however we always aimed to be as transparent as possible so that we wouldn't ever be involved in any litigation……"*

Relevant Documents

- Peaks: PC0146066[37] and PC0146094[38]
- The change, and PO's approval of the change, is documented in OCP 15926[39] and OCP 16010[40]

[37] F/416
[38] F/417
[39] F/417.1
[40] F/418.1

FUJ00155196

3.234 → 3.242

- Old Horizon
- The Peaks[41] referenced by Coyne relate to a property being missing from harvested data
- Coyne (3.239) refers to the fix applied under PC0151724 as using the Transaction Repair Tool.
- It is correct that the Tip Repair Tool (under OCR 17403) was used here, however, as set out below there were a number of later corrections relating to this issue documented under PC0152014.

Background: missing properties

- When a property is missing from a message, its correct value can be determined from other information in the message store. This means that attributes such as product ID and mode are written in the message in multiple places and/ or can be deduced from the other transactions in the session.
- For example:
    - The <mode> property missing from one part of the harvested transaction is also recorded in a different part of the transaction. (DES/GEN/SPE/0007 (disclosed at POL-0153527 but not in the trial bundle) provides a good description of Modes from pages 45 – 51. Counter Modes and Transaction Modes are both described at page 45.)
    - Specifically, the mode is recorded for use by the Riposte system and for the TPS system separately within the same message.
    -
    - As a result of the above, if the TPS <mode> property is missing/ not written, an FJ technician can use the Tip Repair Tool to take this information from the Riposte <mode> property and implement a repair using the Riposte system <mode> property.
- This condition is automatically detected by Horizon validation and notified via overnight reporting. Specifically, the MSU is notified via datacentre generated reports. In the case of PC0152014, the MSU was notified as a result of the TPSC257 - POLFS Incomplete Summaries Report.
- In terms of identifying the root cause, this will depend on the particular property and how it is being used.

What happened?

Peaks: PC0175821[42], PC0151718[43] and PC0152014[44]

- These Peaks experienced the following additional issue as well as the missing properties: settlement records had not been written and would have resulted in a receipts and payments mismatch for the branch if not corrected.
- This required the SSC to:
    - Fix the data feed to Post Office using the Tip Repair tool. This was used to identify the incomplete TPS transaction and passed onto POLFS to correct the back-end TPS database and did not have the ability to impact branch accounts.
    - Insert an additional balancing transaction message into the branch messagestore to avoid a R&P mismatch. The messages included audit information to show they were inserted by the SSC and explain the issue.

PC0175821 F/485

- KEL referenced in the Peak:

[41] PC0152014 [F/432], PC0147357 [F/420], PC0152203 [F/435], PC0151724 [F/430], PC0109649 [F/227], PC0109772 [F/228], PC0114129 [F/244], PC0151628 [F/427] and PC0133933 [F/338]
[42] F/485
[43] F/429
[44] F/432

FUJ00155196

- 19.02.2009: Reference to **KEL obengc3120K**[45] which confirms that Fujitsu should check report TPSC254 for symptoms of there being a problem with messages being written with no corresponding settlement.
- This confirms that "*If the session was settled properly*" – i.e. the transaction took place then "*MSU must raise an OCR so that SSC can use the TIP Repair Tool to populate the missing columns, using values from another transaction for the same currency, same branch, same day if possible*"….. "*By repairing the txn, the TPS_POL_FS_SUMMARIES_INCOMP will be corrected automatically after the txn has been successfully harvested*".
- This KEL obengc3120K then refers to **KEL acha3159Q**[46] which covers another issue involving missing attributes and a missing settlement line and explains that the solution will depend at "*what point the problem is noticed and what has been done at the branch*" and warns that the SSC should not "*make any Harvester or Incomplete Summaries corrections until the problem is fully understood and the strategy for correction has been decided upon and agreed by POL*". This is good as shows the SSC should not be making changes without agreeing them first with Post Office.
- KEL acha3159Q then proceeds to explain the different situations that could be in place, depending upon what action the SPM has taken so far, explaining that it may be possible for the SPM to reverse the 'problem' transaction, without SSC intervention.

Summary of the Peak:

- This Peak not only involves the two separate issues (missing properties and missing settlement lines) but is particularly complex in terms of timing when the transactions were written and what the SPM was doing in the branch too. It appears that some of the corrective action undertaken by Fujitsu in this Peak caused a further harvester exception, although this is not immediately clear. What is clear from this Peak is:
  - Each change involved an OCR and is properly documented
  - Following Fujitsu's corrective action, the branch had no Receipts and Payments mismatch, indicating that there was no discrepancy – i.e. no loss to the branch
  - The branch were aware of the issue.
  - The issue was made more complex to ultimately fix as a result of the manager in branch making an incorrect declaration.
  - A BIMS was issued for audit purposes. Note - we have not searched for this BIMS but it may be that the BIMS assists in terms of answering some of the missing points below, but may also be unhelpful and will generate further disclosure.
- There is no indication in the Peak or OCR that the messages inserted included information to show they were inserted by the SSC, however, OCP 21918 [F/485.2/1] documents that this was formally approved by Post Office and confirms that the SPM was aware of the change "*From speaking to Wendy, the manager in the branch, first thing on Tuesday morning…..is the quietest time for them. I have advised that you will call her as you are about to start and as you finish*".

Peak details:

- 19.02.2009: Peak PC0175821[47] raised as a result of the branch appearing in the TPSC254
- 19.02.2009: OCR 21847[48] raised and approved to use the TRT to repair 5 harvester exceptions
- 19.02.2009: Root cause diagnosed in terms of there being two issues here:
  - The five transactions missing the core data – as resolved by OCR 21847
  - The absence of the equal and opposite settlement lines – with a comparison to PC0152014 (explained in detail below) as being a similar problem

  Confirmation at F/485.1/1 that "*For the first problem, I have used the TRT to insert the missing data i.e. Region, Margin, Margin Product and EffectiveExRate*"
- 20.02.2009: Investigations into the TPS_POL_FS_Summaries_Incomp report results, noting that the total non-zero value for this branch is "£989.96"

[45] Not in trial bundle but disclosed at POL-0036473.
[46] Not in trial bundle but disclosed at POL-0036471.
[47] F/485
[48] F/485.1

FUJ00155196

- 20.02.2009: Session found with a net balance of £989.96, being the session causing the issue. This session involved different currencies being sold with no settlement message written, causing the non-zero amount. Summary extract from the Peak below explaining Fujitsu's findings and why the messages were rejected by the harvester (F/485/2):

```
Date:20-Feb-2009 16:02:57 User:Garrett Simpson
[Start of Response]
After discussion with Cheryl and David I think the situation was this:-
1) The session at 11:52 had four Mode:SC transactions for different currencies. Each one of these messages was missing
mandatory fields so the harvester rejected them. These messages added up to £989.96.
2) The harvester rejections caused the whole day's transactions to go to the incomplete summaries table - without the four
messages rejected by the harvester.
3) The session at 11:52 was missing its settlement message. Its value would have been £-989.96.
4) The result so far is that the summaries incomplete table is short of five messages but its value totals zero.
5) Catherine used the TRT to repair four messages.
6) These four messages were sent to POLMIS in file W_049800.
7) The same four messages were now added to the summaries incomplete table so that now has a sum of £989.96. This will now not
go to POLFS.
Looking at the summaries incomplete table I see 40 rows inserted on 18-Feb and 4 rows inserted on 19-Feb.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 3 hours
```

- 23.02.2009: Fujitsu's investigations then show that the Canadian Dollar transaction of £8.40 was reversed later that day, meaning the total values in the incomplete summaries report was £8.40 (slight revision to point 4 in the Peak extract immediately above).
- 23.02.2009: Confirmation that the branch has a loss of just under £1,000 and that this is even more complicated than first thought.

```
Date:23-Feb-2009 12:20:37 User:Anne Chambers
[Start of Response]
I tried to contact the PM (who has raised 2 calls but been sent to the NBSC) to say it was a system problem. Not available
until tomorrow. The branch has a loss of just under £1000.

This is even more complicated than described above. The set of SC transactions was almost certainly written when a second pouch
reversal (RISP) was initiated (via a barcode scan) before the first was complete. Instead of writing the set of RISP messages,
settled to the 'currency in pouches', it wrote a set of badly formed SC messages with no settlement at all.

These had the sign on the PQty attribute opposite to the sign on the SaleValue (so the stock quantity was reduced but the
stock value increased). When they balanced on 19th Feb, the quantity was corrected via a DDN (and converted to a cash loss) and
there was a large revaluation up. This data has already been fed into POLFS.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
```

- 02.03.2009: OCR 21847 actioned (to resolve and repair the first issue being the missing core data as above)
- 03.03.2009: Confirmation that the four transactions were sent to POLFS
- 06.03.2009: The correction caused a further set of harvester exceptions and incomplete summary lines. Note, it is not clear from the documents why this was the case. However, these further exceptions were dealt with in PC0176680 F/487, which is a very short Peak and simply corrects these 5 harvester exceptions under OCR 21951 F/487.1, which confirms "*5 harvester exceptions were repaired 4th March. The incomplete summaries table was amended 5th March, in the same way as described in OCR 21847, except the signs on the amounts and quantities were all reversed*"
- 06.03.2009: Confirmation that:
  - The branch rolled over on 4 March with the expected R&P mismatch (as the missing settlement lines have not been repaired) but not the gain they should have had.
  - Upon further investigation, it appears that the clerk had declared the currency to match the system figures and not actually the currency on hand.
  - Post Office contacted the manager on 5 March and the manager did another balance with the correct declarations, resulting in a net gain of £10.85.
- 13.03.2009: "*POL agreed to SSC taking corrective measures by inserting messages which caused an equal but opposite effect. Office produced a BT statement on 11-03-2009 which confirm all is right again i.e. no R&Ps mismatch*".
- 20.03.2009: BIMS issued to Post Office for audit purposes.

Branch 183227: PC0152014[49] and PC0151718[50]

FUJ00155196

- 26.11.2007: A $1,000 transaction was written at the branch. Due to a code defect:

  1. Part of the transaction was missing required properties/ attributes
  2. The transaction was written without its associated GBP settlement line

  Part 1: Missing attributes under PC0151718

- 27.11.2007: Peak PC0151718 raised as a result of the branch appearing in the TPSC254 harvester error report because required properties/ attributes were missing from the transaction
- 27.11.2007: OCR 17403[51] raised
- 30.11.2007: Root cause in PC0151718 being identified as missing attributes, extract below

```
Date:30-Nov-2007 12:21:53 User:Catherine Obeng
This is another case where important data from the 'Blackbox' attributes has been left off by the counter code. This missing
information includes: Bureau_Region, Margin, Margin_Product.
```

- 06.12.2007: Fujitsu corrected the missing attributes in the TPS database for the $1,000 transaction using the Tip Repair Tool under OCR 17403. This enabled the TPS system to continue processing the corrected $1,000 transaction. Note, while Fujtisu have confirmed that messages inserted would include information to show that they were inserted by the SSC, there is nothing in the Peak to confirm that this was done.
- 17.12.2007: Peak closed as Incomplete Summaries exception was being investigated under PC0152014

  Part 2: Missing settlement line under PC0152014

- 07.12.2007: Peak PC0152014 raised as a result of the POLFS Incomplete Summaries Report
- 07.12.2007: OCR 17493[52] raised to reduce the USD aggregated total by $1,000/ $484 to make the POLFS feed balance to zero as a result of the missing settlement/ GPB message (N.B. this was approved - see Peak entry 07.12.2007 at 10:41:28). N.B. This change would have been made via SQL in the TPS database using APPSUP privileges.
- 10.12.2007: FJ identified the root cause being the single SC (Serve Customer) line written for $1,000 (£484) with no settlement in the middle – i.e. the transaction was written without its corresponding GBP settlement
- 10.12.2007: OCP 17510[53] raised to deal with inserting a new message on to the Counter to remove the effects of this
- 10.12.2007: FJ inserted an equal and opposite USD transaction onto the counter using this OCP 17510
- 10.12.2007: FJ identified that, due to the $1,000 transaction being written without its corresponding GBP settlement, there would be a R&P mismatch at the office when the branch tried to balance if the issue was not fixed.
- 12.12.2007: OCR 17532[54] raised to add the $1,000 to the aggregated sum of the $US transactions for 11 December 2007, Trading Period 8, Balancing Period 1. This appears to be what confused Torstein in cross examination because the effect of this was to increase the aggregated figure by $1,000 to $2,080. However, all this change was doing was to make TPS/POLFS match Horizon - to remove the negative balancing transaction that Fujitsu had added in OCP 17510. N.B. This change would have been made via SQL in the TPS database using APPSUP privileges. This change would have been to branch data held in the TPS database.
- 12.12.2007: Confirmation that the branch did not have any issues with mismatched transactions, because this was resolved before they rolled over (under OCP 17510 and OCP 17532)

[49] F/432
[50] F/429
[51] F/430.2
[52] F/432.1
[53] F/432.2
[54] F/434.1

FUJ00155196

Master Peak for code fix

- Code fault: "*transaction Mode is missing on the RISP (REM IN Pouch reversal) lines*"
- Issue was considered to have a low rate of occurrence and not fixed

Peaks evidencing general repairs for missing mode

- PC0152203: Harvester Exception occurred as a result of an incomplete record. This was corrected using the Tip Repair Tool under OCR 17550.
- PC0151628: Harvester Exception occurred as a result of an incomplete record. There was an issue with the repair as follows:
    - The SSC selected the wrong mode when correcting the record using the Tip Repair tool
    - This led to a further Peak PC0151724 (explained directly below) being raised in order to "*repair the missing transactions into POLFS*". This is a good example of how the system has multiple levels of checks so that even if a user error occurs it is likely to cause a further exception.
    - In this particular instance, as the issue related to files being sent to POLFS, the mode did not matter.
- PC0151724[55]: The data sent was correct and Peak confirms (27 November 2007 entry) that the mode was irrelevant for the cash transactions in POLFS
- PC0109649[56]: Harvester Exception fixed. Under change control

Impact on branch accounts

- Correction of harvester exceptions which simply involve missing properties/ attributes (i.e. some required data) involves the use of the Tip Repair tool to fix the data feed to Post Office, as explained above. This was used to identify the incomplete TPS transaction and correct the back-end TPS database. This was entirely back-end and would not affect branch accounts.
- Corrections of harvested data alone requires no intervention in the message store and are repaired in order to provide data that passes validation for overnight processing and subsequent transmission to Post Office systems.
- Where there is a missing settlement value, the fix involved the insertion of a balancing transaction into the branch messagestore to avoid a R&P mismatch. This would have the ability to affect branch accounts, however, the messages included audit information to show they were inserted by the SSC and explain the issue.

Analysis

- **Coyne (3.234)** quotes PC0152014[57] (being one of the peaks that had the settlement records issue detailed above) as follows: "*…the first issue has been corrected by inserting a message into the messagestore, for equal but opposite values/ quantities as agreed with POL*". Coyne proceeds to note **(3.236)** that this indicates that there has been more than one Balancing Transaction applied within Horizon. Coyne is mis-using the word "balancing transaction" in his report – this instance does not refer to the use of the "balancing transaction" referred to by Godeseth at para 58 of his first witness statement. This was not the injection of a whole transaction. Rather, in PC0152014 an additional equal and opposite USD transaction onto the counter under OCP 17510.
- **Coyne (3.239)** notes that the fix applied to the data in PC0151724[58] was initially set to the wrong Transaction Mode ID. Fujitsu have confirmed this is correct and was as a result of human error. This issue was automatically detected by the TPSC257 Incomplete Summaries Report. If this issue had not been automatically detected and had not been corrected, the branch data for that full day would not flow through to POLSAP. This would lead POLSAP to raise a call and the issue corrected.

[55] F/430
[56] F/227
[57] F/432
[58] F/430

FUJ00155196

- The comment in the below entry from PC0152014 that "*this may also have caused a receipts and payments error*" is not correct. Fujitsu have confirmed that this is actually a standard template that is included on calls raised against this report as a reminder to check for this scenario. In actual fact, this issue would have caused a R&P mismatch when the branch balanced, but as explained above, the issue was resolved before a R&P mismatch could occur.

```
Date:07-Dec-2007 10:33:16 User:Claire Drake
TPSC257 - POLFS Incomplete Summaries report produced on 06/12/2007.
Report shows 1 entry for Branch 183227.

This branch does not appear in the TPSC254 (Harvester error report) and TPSC250 (Host Detected Transaction Control Errors)
report.

KEL surs448L / garrett835Q may be relevant. Relevant report attached.

**This may also have caused a receipts and payments error, can EDSC please confirm whether this is a gain or loss at the
counter and the amount.**
```

- **OCP 17150**: Steve Parker's team believe this action was taken on the assumption that the first $1000 transaction did not actually take place at the branch (i.e. the clerk did not complete it due to the system error). Note:
    - If that assumption was correct, there would be no discrepancy in the branch (i.e. the Horizon record would have matched what happened in the branch).
    - If that assumption was incorrect, there would still be no loss in the branch. Although the branch holding of $ would be 1000 lower than the system (because the injected transaction increased the Horizon derived USD figure), there would be an equal and corresponding increase in the GBP/Cheque held by the branch (because of the settlement that was taken by the branch for the USD transaction and was not recorded on Horizon due to the injected transaction).

- During Torstein's cross-examination, Green referred to the 14 December entry from **PC0152014** (extract below) and asserted that the injection by the SSC caused a discrepancy.

```
As a result of this corrective action, the net effect on POLFS is zero, and POLFS figures are in line with the branch. POLMIS
received both the original message and the corrective message.
```

- What appears to have confused Torstein during his cross-examination is the OCR 17532, which states:
  "*Updated POLFS feed for branch 183227 product 5129 mode SC with SaleValue=1014.73 and PQty=2080*"
  Sale Value is the GBP value, PQty is the dollar amount.
- The effect of the above was to increase the aggregated figure by $1,000 to a total of $2,080. However, all this change was doing was to make TPS/POLFS match Horizon and to remove the negative balancing transaction that Fujitsu had added in OCP 17510.
- Fujitsu have advised that this transaction was inserted into the counter to ensure that TPS harvested it correctly. Note that this is not referred to in Parker 2 or our letter to Freeths regarding the additional 10 Peaks where data was injected into the counter.

Relevant Documents

- PC0175821 [F/485], OCRs/ OCPs referred to: OCR 21847[59] and OCP 21918[60]
- PC0152014 [F/432], OCRs/ OCPs referred to: OCR 17532[61], OCP 17510[62], OCR 17493[63]
- PC0147357[64], OCRs/ OCPs referred to: OCP 17510[65], OCR 17532[66] and OCR 16225[67]

[59] F/485.1
[60] F/485.2
[61] F/434.1
[62] F/432.2
[63] F/432.1
[64] F/420
[65] F/432.2

FUJ00155196

- PC0152203 [F/435], OCR referred to: OCR 17550[68]
- PC0151724[69], OCR referred to: OCR 17409[70], KELs referred to: Surs448L and Garrett835Q – neither are in the trial bundle but both are in the bundle of KELs prepared for Counsel
- PC0109649 [F/227], PC0109772 [F/228], PC0114129 [F/244],
- PC0151628 [F/427], OCR referred to: OCR 17382[71]
- PC0133933 [F/338]
- KELs: GillR269R [F/679.1], CObeng2634M [POL-0035136]
- First witness statement of Torstein Godeseth [E2/1]
- Host BRDB Transaction Correction Tool Low Level Design [F/425]
- Branch Database High Level Design, DESAPPHLD0020 [F/1786], specifically F/1786/52 and the section 'BRDB Transactions to TPS', which explains Harvester Exceptions.

3.243 → 3.246: TIP Repair Tool

- Old Horizon
- Coyne refers to 3 peaks which all relate to the ordinary use of the TIP Repair Tool referenced at para 60 of Godeseth[72].
- As documented in Godeseth, changes made using the TIP Repair Tool do not change the transaction data used by branches but back-end data in the separate TPS system used by Post Office.
- There could therefore be no impact on branch accounts.

Background: TIP Transaction Repair Tool

- As per Torstein 1[73] and 3[74], this tool can only be used on data that has failed to be delivered between the correspondence servers in Legacy Horizon and the TPS system because it is missing a mandatory/ key attribute;
- This tool was developed to repair TPS transactions that fail validation
    - This is described in document PI/MAN/001[75]
    - TPS checks the validity of each record, section 3 of the document has a list of possible reasons why a record may fail validation:
    - The possible reasons as to why an insert fails are following:
        - Value of a mandatory (NOT NULL) column is missing from the TPS transaction tables.
        - Value of a column from the TPS Transaction tables is not in the range expected, e.g., value of “Reversal Indicator” is not among ‘0’, ‘1’ and ‘2’.
    - The tool provides the record fields available and highlights those that are missing/incorrect.
    - The SSC would then enter the correct value for those fields and save the change ready for overnight processing.

- The correction is made on the TPS database and cannot directly affect the branch accounts in the Correspondence Servers in Legacy Horizon.

What happened?

[66] F/434.1
[67] POL-0500185
[68] POL-0501504
[69] F/430
[70] POL-0501357
[71] POL-0501324
[72] E2/1/18
[73] E2/1/18
[74] E2/14/3
[75] This document describers how to use the tool to repair the transactions and essentially serves as a user guide to accompany the TIP Transaction Repair tool. All versions disclosed. 2 versions in the trial bundle: 2017 version: F/1598 and 2011 version: F/88.1

FUJ00155196

Peak PC0159702[76]

- 06.06.2008: Peak opened as a result of 3 new exceptions showing on the Harvester Exception report. This report is run automatically each day.
  06.06.2008: TIP Transaction Repair Tool used to "*repair the START_DATE/START_TIME_FRACTION and the END_DATE/END_TIME_FRACTION from NULL to valid values for the 3 txns on 05-Jun-2008 for this branch*."
    - This is documented in OCR 19367[77]
- 09.06.2008: Confirmation that the transactions were successfully harvested ie transferred from TPS to other PO systems.
- 09.06.2008: Peak closed. SPM not aware of any of this because irrelevant to them.

Peak PC0159759[78]

- 09.06.2008: Peak opened as a result of 4 new exceptions showing on the Harvester Exception report;
- 09.06.2008: Root cause identified as: code omitted mandatory fields including the start date, start time fraction, end date and end time fraction for 4 messages. Fujitsu used the tool to insert the suitable values. Confirmation that these "*should go to POL this evening*".
    - Documented in OCR 19384
- 10.06.2008: Peak closed.

Peak PC0159445[79]

- 02.06.2008: Peak opened as a result of a large number (4,364) of exceptions being generated on the same day.
- 02.06.2008: Root cause identified: large number of exceptions caused by 2 changes to the TPS harvester[80]. Development produced an SQL script to repair the rejected transactions because there were too many for a manual repair.
- 04.06.2008: Confirmation that the SQL script will need to first be tested on the Live Support Testing database before being applied to live
- 06.06.2008: Confirmation that the SQL script has successfully repaired the 4,364 transactions.
- 10.06.2008: Peak closed.

Impact on branch accounts

- None.

Analysis

- Coyne correctly identifies the three Peaks as arising from automated reports, but these are not "reconciliation reports" as he calls them. There is no reconciliation of data (ie. no comparison). The report is generated by the TPS system which checks the data against a set of pre-defined rules.
- Coyne quotes from PC0159759 as follows "*That stupid mail code….I have used the TRT to insert suitable values…*" In terms of responding to this:
    - Reference to "stupid mail code" reflects the frustrations involved when resolving issues as part of the support team;
    - The "suitable values" that were applied were done so in TPS as described above.

Relevant Documents

[76] F/458
[77] F/458.1
[78] F/459
[79] F/456
[80] These changes are explained in detail in the Peaks

FUJ00155196

- PC0159445 [F/456], OCPs/ OCRs referred to: OCP 19369[81], OCR 19304[82]
- PC0159702 [F/458] and PC0159759 [F/459]
- First and third witness statements of Torstein Godeseth [E2/1/18] and [E2/14/3]
- Branch Database High Level Design, DESAPPHLD0020[83] (multiple versions disclosed)
- OCR 19367 [F/458.1] and OCR 19384 [F/459.1]

[81] POL-0503251
[82] POL-0503197
[83] 2018 version: F/1786

FUJ00155196

3.247 → 3.248: TIP Repair Tool

- Old Horizon.
- Coyne has misunderstood Peak PC0172841[84]. The Peak is discussing issues with data in the TPS system, not in Horizon.
- This made clear through multiple references to activity happening in "TPS" and using the "TIP Repair Tool". Also:
  - The second to last entry on the Peak states "*I have checked the live TPS database. The table has been amended as I suggested*".
  - The fix that was rolled out is described as "1 TPS patch file" – see entry on 22 Jan 2010 @ 12:23:08
- As all this activity happened in the TPS database, there was no impact on the branch accounts in Horizon.

What happened?

- 08.01.2009: Peak raised
- 08.01.2009: Issue with premature archiving identified
- 20.01.2010: Fix proposed to avoid transactions effectively being lost[85]
- 10.03.2010: Live support testing of fix
- 13.07.2010: Fix applied to live (Release Peak: PC0197557[86])

Impact on branch accounts

- None – all activity happened in the TPS database.

Analysis

- **Coyne (3.248)** *notes that this Peak "indicates that Fujitsu support had the capabilities to manually rebuild data".*
- This peak documents the discovery of an issue with a parameter in the TPS archiving process that was in turn fixed formally by development.

Relevant Documents

- Peaks: PC0172841 [F/564] and PC0197557 [POL-0367433]
- TIP Transaction Repair User Guide, PI/MAN/001 [All versions disclosed. 2 versions in the trial bundle: 2017 version: F/1598 and 2011 version: F/88.1]
- First witness statement of Torstein Godeseth [E2/1]
- Branch Database High Level Design, DESAPPHLD0020 [2018 version: F/1786]

[84] [F/564]
[85] Note, the actual transactions would not be lost. What would be lost/ removed would be the copy of the transaction that was held in the repair tables within the TPS which is what is then accessed by the TIP repair tool. This would mean that the transaction would no longer be visible to the TIP repair tool and could not be repaired.
[86] [POL-0367433]

FUJ00155196

SECTION 2: DATA REBUILDING: PARAS 3.249 – 3.265

In this section there are two discrete issues:

- Para 3.249 – PEAK PC0057909[87]
- Para 3.263 – PEAK PC0197987[88] (note – although this is dated April 2010 it relates to a terminal that is still running Old Horizon because this occurred during Horizon Online roll out)

Paragraph 55.4 of Parker 1[89] describes the process in Old Horizon for re-building data.

- In old Horizon, data was held locally on terminals in branches.
- The terminals would automatically replicate data between them, so that multiple back-up copies of the same data were kept.
- It is of course possible for a terminal to break (burnt out hard-disk) or data to be corrupted. In that event, the corrupted data is deleted in full and the automatic processes within Horizon that replicate a correct copy from another terminal.
- This Section of Coyne's report does not directly apply to Horizon Online because data is not held locally in branch. However, the same risk applies to data held in a data centre as there could be a disk failure or corruption on a server. Ordinary data centre support includes backing-up servers and recovering data from back-ups.

3.249 → 3.262

Summary

- Old Horizon
- This issue relates primarily to an incident at a single branch.
- It only mentions data rebuilding in the sense already described in Parker 1.
- In fact, the data rebuild in this case was only floated as a possibility but did not actually happen because an alternative solution was found by working with the SPM.
- Generally, Coyne has selectively quoted from the relevant Peaks and his account is tendentious.

Note:

- This incident is spread over several Peaks. One needs to read though the Peaks chronologically to see the full story.
    - PC0057909[90] is the original Peak
    - This is then cloned to PC0058435[91] due to an unrelated problem with associated call logging software. This Peak closes out the branch issue.
    - A further Peak is then cloned from PC0058435 to deal with any related customer issues: See PC0059052[92].

Dates

PC0057909 F/73

- 14 November 2000: SPM raises issue with FJ relating to missing transactions. Specifically:
    - When the SPM did her daily reports after having a new base unit fitted, she noticed missing transactions

[87] F/73
[88] F/628
[89] E2/11/16
[90] F/73
[91] F/74
[92] F/75

FUJ00155196

  - SPM re-entered the missing transactions, correcting her daily reports
  - SPM printed off the balance report all of the missing transactions were showing twice
- 14 November 2000: SPM advised by FJ to contact NBSC
- 15 November 2000: SPM advised by NBSC to remain in CAP 34 until the issue is resolved
- 20 November 2000: FJ ask for more info from SPM on affected transactions
- 23 November 2000: Peak cloned to new Peak PC0058435

PC0058435 F/74

- 23 November 2000: Root cause determined to be bug in Horizon.
- 23 November 2000: Message stores analysed from the Counters in branch and the correspondence server and FJ confirmed:
  - Messagestore on Counters 2 and 3 matched
  - Messagestore on the correspondence server matches Counter 1
  - Messagestore on Counter 1 had 48 messages that did not appear in Counters 2 and 3
  - Messagestore on Counters 2 and 3 had 48 messages that did not appear in Counter 1
  - As a result of the above, when the SPM undertakes a balance snapshot on Counter 1, a different result is produced to Counters 2 and 3
- 23 November 2000: Peak cloned due to problems with the OTI[93]
- 23 November 2000: Development asked to investigate whether there is a deficiency in Riposte and what can be done to stop the issue happening again
- 23 November 2000: Potential option of rebuilding the data considered – i.e. inserting the missing messages onto counter 1, where the failure in Riposte occurred
- 28 November 2000: SPM advised to roll over on counter 2 or 3, but not counter 1
- 29 November 2000: SPM confirmed her APS report[94] was out by £150.21 which related to the two 'AP' transactions that were recovered and reversed on Counter 1. SPM confirmed she has recovered these 2 transactions on counter 2 and that her APS report is now correct. The APS report was incorrect it didn't take into consideration the missing transactions. This wasn't a fault of the APS report, but was a symptom/ as a result of the issue mentioned above in terms of Counter 1 not matching with Counters 2 and 3. There was nothing wrong with the SPM's accounts, rather the APS report gave the SPM an indication that there was a problem here, helping the SPM to identify the issue that the Counters were out of sync.
- 29 November 2000: SPM raised concern that client may have been paid twice (by POL, not by the branch)
- 1 December 2000: Peak cloned to new Peak PC0059052

PC0059052 F/75

- 10 January 2001: Confirmation that there do not appear to be any reconciliation errors (client/ POL reconciliation)

What happened?

- SPM had a terminal in branch swapped out.
  - It was the gateway terminal that was changed.
  - In a multi-terminal branch, one terminal is the gateway and connects to the data centre and the slave counters. The other terminals (slaves) connect to the gateway and each other. The gateway then sends all the branch transaction data to the data centre. Note, this transfer of data happens whenever there is a connection to the datacentre. The gateway is periodically connected to the datacentre during the day (at least hourly) and replicates outstanding messages.
- The new terminal should have automatically replicated data from the one of the other 2 slave terminals in branch.

[93] OTI is the way in which different help desks communicate. FJ have confirmed that a problem with the OTI could have prevented an update being sent back to PinICL, so the Peak was cloned.
[94] Automated Payment Services report produced locally in branch.

FUJ00155196

- Instead, due to the other counters not being connected to it[95], the gateway terminal was installed at 12:04 but did not connect to either terminal/ slave until 15:30. When building a counter, the gateway terminal attempted to connect to all of its neighbours, however, in this case could only connect to its server neighbour. In the meantime, the gateway had completed replication from the data centre and wrote a further 48 messages. However, you are unable to perform new transactions until replication is considered to be complete by riposte – i.e. the gateway has received all messages from all connected neighbours.
- This caused the Gateway counter to get out of sync with Counters 2 and 3.
- The full description of what happened is in Peak PC0058435[96]:

Date:**23-Nov-2000 09:28:00** User:**Richard Coleman**
The messagestores directly from counters 1 and 2 have been extracted.
The messagestore on the Cor Server matches counter 1.
The messagestore on counter 2 has 48 messages which are not on counter 1, and vice versa.
The messagestore on counter 3 matches counter 2.

What I think has happened is this:
1. Engineer replaced Gateway, but it couldn't talk to counters 2 or 3 so it replicated from the Cor Server.
2. The Cor Server was not up to date, and only had messages up to 1-510415.
3. So far so good, but the Gateway still couldn't talk to the other counters and the PM started recovering some AP transactions.
4. By the time the Gateway could talk to the other counters, the messages on the new Gateway were up to 1-510463.
5. Because this number matched the number that the other counters had for the Gateway, there were no messages for the Gateway to catch up on.
6. The messages on the Gateway from 1-510416 to 1-510463 are different from the messages that counters 2 and 3 have for the Gateway.
7. This would explain why doing a balance snapshot on counter 1 produces different results from counters 2 and 3

How was it fixed?

- This issue was not detected by any automatic reporting. Spotted by SPM.

[95] Probably as a result of the network cable being disconnected.
[96] F/74

FUJ00155196

- Instructions were given to the SPM on how to recover the missing transactions in branch. PC0058435[97] says:

  Date:29-Nov-2000 10:11:00 User:Richard Coleman
  Spoken to the PM and and her APS report was out by £150.21 which were 2 transactions that she recovered and reversed on counter 1. She has recovered them again on counter 2 and her AP is now correct. AP numbers 014962 and 014963.

- Limited to one branch as related to hardware issue in branch but note Jenkins comment in PC0058435[98]:

  Date:**11-Dec-2000 17:54:00** User:**Gareth Jenkins**
  I don't know that I can add anything useful here. This is another example of recovery having gone wrong after a box swap.

- Elsewhere there is reference to another Peak PC0052823[99] (Coyne @ 3.258) that deals with the underlying issue so this clearly affected other branches.

  Date:**11-May-2001 08:49:00** User:**Angela Shaw**
  This fix needs bringing forward before S10 for this problem. There have been 20-25 reported occurrences of this problem type recently, which causes receipts and payments mismatches.

- Comment from FJ: Other than providing more guidance to the Engineers replacing counters there was nothing centrally that Fujitsu can monitor. It was up to the postmaster to report differences in his reports on different counters.

- The fix did not get rolled out until September 2002. It looks like it was a difficult issue.

Impact on branch accounts

- Yes – transactions were only available on certain counters, meaning performing a report on counter 1 could have a different result than on counter 2. This meant that when the SPM came to rollover on the counter with the issue, it could cause shortfalls or surpluses.

Analysis

- This is not an example of data re-building. Coyne has used this incident because it allows him to quote the following which is colourful language from FJ:

  Date:**23-Nov-2000 09:33:00** User:**Richard Coleman**
  Can development please investigate on whether there is a deficiency in Riposte and what can be done to stop this happening again.

[97] F/74
[98] F/74
[99] F/54

FUJ00155196

> Also, need advice on how to get the messagestores in sync and to include the missing transactions. I suspect we will need to **trash the messagestores** on counters 2 and 3 and insert the missing messages onto counter 1 (or can the PM get away with inputting the transactions). Some of the ransactions are APS.

- FJ say that "trashing the messagestores" is just casual language used by FJ to mean the same as Parker 1 @ 55.4 ie. delete the message stores and allow them to replicate as normal.
- Coyne also knew that there was no data re-building as he acknowledges this in para 3.249 and 3.259 where he describes the SPM recovering the transactions.
- The relevant extract from PC0058435[100] is:

Date:**28-Nov-2000 15:47:00** User:**Richard Coleman** I have spoken to the PM and advised her to roll over on counter 2 or 3, not 1. But have not mentioned about recovering the AP transactions. Can development please advise on whether the PM does need to recover the AP transactions, since the PM recovered the transactions and then reversed them. If she balances on counter 2 will it take the AP transactions from it's copy or will it only look at AP transactions done on counter 2?
Date:**28-Nov-2000 16:15:00** User:**Lionel Higman** The Call record has been transferred to the Team: Escher-Dev Hours spent since call received: 0 hours
Date:**29-Nov-2000 10:11:00** User:**Richard Coleman** Spoken to the PM and and her APS report was out by £150.21 which were 2 transactions that she recovered and reversed on counter 1. She has recovered them again on counter 2 and her AP is now correct. AP numbers 014962 and 014963. PM is concerned that the customer may be paid twice. I will check the APS files in the morning and clone another call to pass to MSU for reconciliation if this is the case. PM is also concerned that on the Balance snapshot the cheque value is wrong. Her cheque listing is okay, and I advised her to see whether the system will allow her to roll over once cheques have been remmed out, and to contact the NBSC for advice on rolling over. PM is happy for the moment, see what happens tonight.

- Coyne @ 3.251 and 3.252 tries to make it look like FJ just puts this down to user error and ignores the real problem. What his report omits to include are the steps taken by FJ in between his selective quotations
  - Coyne @ 3.251 notes that the first Peak was closed as user error – a code "*40 General – User*". The full extract is below.
  - Fujitsu have confirmed that the 'defect' cause was set to '40 General - User' at the time as Fujitsu did not have enough evidence from the SPM to investigate further. It is not necessarily a 'fair' criticism as all that this is saying from Fujitsu's perspective is that they do not have enough evidence from the SPM. This is therefore not an indication that the SPM caused the problem, although on plain reading of the

[100] F/74

FUJ00155196

wording used we can see why Coyne draws this conclusion. The usual procedure where further evidence is needed would be for the Peak's status to be updated in this way and closed and then for the Peak to be re-opened once the additional information had been provided by the SPM.
    - As can be seen from the below extract, the Peak was actually closed as 'Category 96' – being Insufficient Evidence to gather more evidence.
    - Ordinarily the usual procedure would be for the Peak to be reopened once the additional information had been obtained from the SPM, however, due to the OTI problem, the Peak was cloned.
    - In the cloned Peak, following Fujitsu's further investigations, the defect cause was updated to shoe 'Development – Code'.

- Peak closure categories
    - In terms of why there are only codes 60 onwards described in F/823/23 – End to End Application Support Strategy, Fujitsu have confirmed that this is because this table/ document only references the 'Peak closure categories'.

- Peak 'defect' cause categories
    - Note these are different from the 'Peak closure categories'[101] as 'defect' cause categories illustrate the interim diagnosis/ root cause analysis.
    - Code '40 – General – User' is one of these 'defect' cause categories.
    - Fujitsu have confirmed that they do not believe these defect cause categories are documented in a design document but have provided us with a list that was extracted from the table of options from the database.
    - Fujitsu have confirmed that the information in the Peak when the Peak is being updated shows the category number and the relevant contemporary narrative that is subject to interpretation.
    - Fujitsu has provided the current contemporary narrative for Code '40 – General – User': being 'A fault caused by any user action'. In terms of obtaining a copy of a document that describes this code, we understand that, while Fujitsu is able to extract the codes and provide an explanation of the codes commonly used, including this Code 40, Fujitsu is not aware of a document that contains these codes

```
Date:20-Nov-2000 16:29:00 User:Richard Coleman
F} Response :
Have had a look at the messagestore and am unable to match what the PM is
saying in this call with what I see in the messagestore.
Please provide date and time of the balance snapshot and trial balance
reports that the PM is querying.
Also require quantities and values for the Giro deposits, Green giros and TV
licences on balance snapshot and trial balance.
Require session id's for the transactions that the PM re-entered.
Require dates and times of the daily reports, quantities and values of the
total on each report as well please.
PM has not been contacted, closing as insufficient evidence.
[END OF REFERENCE 23077138]
Responded to call type L as Category 96 -Insufficient evidence
Hours spent since call received: 0 hours
Defect cause updated to 40:General - User
CALL PC0057909 closed: Category 96, Type L
The response was delivered to: PowerHelp
```

    - 3 days later the following is recorded in the Peak that clearly shows that FJ has got more info from the SPM and is investigating further. Coyne omits this quote from his report.

```
Date:23-Nov-2000 09:21:00 User:Richard Coleman
I have spoken to the PM last night and advised that this is being looked
```

FUJ00155196

```
into.
```

```
Date:23-Nov-2000 09:28:00 User:Richard Coleman
The messagestores directly from counters 1 and 2 have been extracted.
The messagestore on the Cor Server matches counter 1.
The messagestore on counter 2 has 48 messages which are not on counter 1,
and
vice versa.
The messagestore on counter 3 matches counter 2.
What I think has happened is this:
1. Engineer replaced Gateway, but it couldn't talk to counters 2 or 3 so it
replicated from the Cor Server.
2. The Cor Server was not up to date, and only had messages up to 1-510415.
3. So far so good, but the Gateway still couldn't talk to the other counters
and the PM started recovering some AP transactions.
4. By the time the Gateway could talk to the other counters, the messages on
the new Gateway were up to 1-510463.
5. Because this number matched the number that the other counters had for
the
Gateway, there were no messages for the Gateway to catch up on.
6. The messages on the Gateway from 1-510416 to 1-510463 are different from
the messages that counters 2 and 3 have for the Gateway.
7. This would explain why doing a balance snapshot on counter 1 produces
different results from counters 2 and 3.
```

- Coyne then says at 3.252 that "despite the diagnosis there still appears to be unknowns". He quotes the outstanding queries flagged by FJ on 23/11/2000 @ 9:33 but does not quote the entry immediately beforehand at 9:28 quoted above that explains that F problem resulting in counter 1 producing different results from counters 2 and 3. While Fujitsu still needed to investigate the underlying root cause, it is clear from the above extract that they had understood and determined the full scope of the issue.

```
te:23-Nov-2000 09:33:00 User:Richard Coleman
Can development please investigate on whether there is a deficiency in
Riposte and what can be done to stop this happening again.
Also, need advice on how to get the messagestores in sync and to include the
missing transactions. I suspect we will need to trash the messagestores on
counters 2 and 3 and insert the missing messages onto counter 1 (or can the
PM get away with inputting the transactions). Some of the transactions are
APS.
Also how will this affect their balancing. They are currently in CAP 34.
Thank you.
The Call record has been transferred to the Team: QFP
Defect cause updated to 14:Development - Code
Hours spent since call received: 0 hours
```

- The full extract from the Peak looks like the below. He could not have missed he key bit which he has omitted.

```
Date:20-Nov-2000 16:29:00 User:Richard Coleman
F} Response :
Have had a look at the messagestore and am unable to match what the PM is
saying in this call with what I see in the messagestore.
Please provide date and time of the balance snapshot and trial balance
reports that the PM is querying.
Also require quantities and values for the Giro deposits, Green giros and TV
licences on balance snapshot and trial balance.
Require session id's for the transactions that the PM re-entered.
```

FUJ00155196

Require dates and times of the daily reports, quantities and values of the total on each report as well please.
PM has not been contacted, closing as insufficient evidence.
[END OF REFERENCE 23077138]
Responded to call type L as Category 96 -Insufficient evidence
Hours spent since call received: 0 hours
Defect cause updated to 40:General - User
CALL PC0057909 closed: Category 96, Type L
The response was delivered to: PowerHelp

Date:**23-Nov-2000 08:52:00** User:**Richard Coleman**
CALL PC0058435:Priority C:CallType C - Target 30/11/00 08:52:09
Call PC0058435 cloned from original call PC0057909

Date:**23-Nov-2000 08:53:00** User:**Richard Coleman**
Call has been cloned due to problems with the OTI.
Target Release updated to CSR-CI4R
CALL PC0058435:Priority B:CallType C - Target 28/11/00 08:52:09

Date:**23-Nov-2000 09:20:00** User:**Richard Coleman**
New evidence added - Event logs for counters 1 and 2
New evidence added - Messagestores for counters 1 and 2

Date:**23-Nov-2000 09:21:00** User:**Richard Coleman**
I have spoken to the PM last night and advised that this is being looked into.

Date:**23-Nov-2000 09:28:00** User:**Richard Coleman**
The messagestores directly from counters 1 and 2 have been extracted.
The messagestore on the Cor Server matches counter 1.
The messagestore on counter 2 has 48 messages which are not on counter 1, and
vice versa.
The messagestore on counter 3 matches counter 2.
What I think has happened is this:
1. Engineer replaced Gateway, but it couldn't talk to counters 2 or 3 so it replicated from the Cor Server.
2. The Cor Server was not up to date, and only had messages up to 1-510415.
3. So far so good, but the Gateway still couldn't talk to the other counters and the PM started recovering some AP transactions.
4. By the time the Gateway could talk to the other counters, the messages on the new Gateway were up to 1-510463.
5. Because this number matched the number that the other counters had for the
Gateway, there were no messages for the Gateway to catch up on.
6. The messages on the Gateway from 1-510416 to 1-510463 are different from the messages that counters 2 and 3 have for the Gateway.
7. This would explain why doing a balance snapshot on counter 1 produces different results from counters 2 and 3.

Date:**23-Nov-2000 09:33:00** User:**Richard Coleman**
Can development please investigate on whether there is a deficiency in Riposte and what can be done to stop this happening again.
Also, need advice on how to get the messagestores in sync and to include the

FUJ00155196

```
missing transactions. I suspect we will need to trash the messagestores on
counters 2 and 3 and insert the missing messages onto counter 1 (or can the
PM get away with inputting the transactions). Some of the transactions are
APS.
Also how will this affect their balancing. They are currently in CAP 34.
Thank you.
The Call record has been transferred to the Team: QFP
Defect cause updated to 14:Development - Code
Hours spent since call received: 0 hours
```

- **Coyne @ 3.262 –** he is correct that this incident may have stretched over three cash account periods. Note – CAPs are weekly. This situation lasted 15 days.
- **Coyne @ 3**.261 comments that customers may have been impacted. This is irrelevant in this litigation as this would have no bearing on branch accounts.

Questions

a) What was actually proposed here? Which counters would have been deleted and which counters' data would have been replaced?

48 messages

These 48 messages would have included the 2 APS transactions detailed in the Peak. Note that messages can be information other than transactions, which would explain why there were so many messages but only 2 transactions. As such, broadly speaking we can say the 48 messages relate to the 2 APS transactions.

To recap:

Counters 2 and 3 were missing 48 messages from Counter 1.
Counter 1 was missing 48 messages from Counters 2 and 3.
The correspondence server:

- had the 48 messages from Counter 1
- did not have the 48 messages from Counters 2 and 3
- in relation to the remaining messages/ transactions, after the 48 messages, the Counters were in sync so all remaining messages were correctly replicated between the Counters and to the correspondence servers

The proposition, as documented in PC0058435 F/74, was to delete the message stores on Counters 2 and 3 and allow them to re-replicate as normal from the server. This 'Trashing' of the messagestore from Counters 2 and 3 would have:

- forced a replication of everything (including the Counter 1 missing 48 messages) onto Counters 2 and 3
- bought Counters 2 and 3 into agreement with the correspondence server and Counter 1
- deleted the 'stuck' messages on Counters 2 and 3

The result will leave the 48 stuck messages on Counters 2 and 3 having not been written. These would need to have been entered manually (either by the SPM or introduced via an import by FJ using the original transaction messages held on Counters 2 and 3).

While the above solution was proposed, there is no evidence in the Peak that trashing actually happened here.

b) What was the alternative solution that was adopted?

On 29 November 2000 the SPM confirmed her APS report was out by £150.21, which related to the 2 'missing' transactions that she re-entered and reversed on Counter 1 and related to the 48

FUJ00155196

missing messages from the Counter 1 messagestore. Instead of FJ intervening as above by re-replicating the messages on the Counters, the SPM recovered the 2 missing transactions on Counter 2 and her APS report was then correct. While the SPM was concerned that the client would have been paid twice, this would have been a reconciliation issue between POL and the client and therefore would have been entirely separate to the branch.

What is unclear and a point to discuss during our call with FJ is whether or not the stuck 48 messages from Counters 2 and 3 would have been resolved from the above. It would appear not.

c) **Why did the peak say "closing as insufficient evidence"?**

The Peak was closed as Fujitsu required further information to investigate – this will be the 'insufficient evidence'. Fujitsu have confirmed that the normal process would be for the original Peak to be re-opened with the additional information, however, due to the issue with the OTI, the Peak was cloned to allow continued investigation. The Peak was then cloned to a new Peak PC0058435 where the further evidence was provided and Fujitsu's investigations continued.

d) **The peak refers to problems with the OTI. What is the OTI and why would problems with the OTI have caused the peak to be cloned?**

OTI is the way in which different help desks communicate – i.e. the path/ connection between the different ticketing systems. In this case there was a problem where the call in peak could not be re-opened remotely from the other ticketing system (via the OTI) so Fujitsu reopened the issue by cloning the Peak.

Relevant Documents

- Peaks: As described above.
- Parker 1 @ 55.4 [E2/11/16]

3.263 → 3.265

Summary

- Although dated April 2010, this Peak relates to an Outreach branch running old Horizon.
  - Peak states: *2010-04-20 14:33:58 [Hale, Perry]: Pm states the Kit will be back at the main branch at 17:00 tonight PM states the kit will leave for the outreach at 09:00 and returns at 16:00 tomorrow.*
  - This shows the kit is mobile and an outreach.
- FJ have confirmed that this is an old Horizon issue – by April 2010 HNG-X was still being piloted so some branches would have been on Old Horizon.
- In a one counter branch (like an outreach) there is a second hard-disk in the terminal used to back-up the main hard-disk (the mirror disk). A back-up is also made overnight to the correspondence servers.
- This SPM's mirror-disk was broken and the terminal was not connecting to the data centre.
- SPM was advised not to trade until problem fixed because if the main hard-disk failed there would be no back-up and therefore a risk of loss of transaction data. This was a warning against a data loss happening – there is no evidence in the peak that this actually happened.
- PC0197987[102] (which is very short) refers to:

Date:**20-Apr-2010 15:04:42** User:**Kevin Miller**
[Start of Response]
Ripostemirror service is not working.

[102] F/628

FUJ00155196

Unable to connect to counter to attempt manual rebuild as counter is on site.

- FJ have confirmed that the reference to "manual re-build" means the form of data rebuilding described in Parker 2 @ 36.
- Coyne's conclusion @ 3.265 is correct if he means the same as Parker, but he is unclear as to what he is referring.

FUJ00155196

SECTION 3: DATA DELETION: PARAS 3.266 – 2.276

In this section there are four discrete issues:

- Para 3.266 – PC0241528[103]
- Para 3.270 – PC0234786[104]
- Para 3.271 – PC0263716[105]
- Para 3.275 – PC0197592[106]

All four relate to Horizon Online. Coyne relies on all four to show that FJ delete BRDB data. This is correct, but his view is not precise enough. FJ is not deleting transaction data but other data in the BRDB that does not impact on the branch accounts.

In relation to each issue above.

- Issue 1 – FJ are deleting data from the BRDB but not transaction data.
- Issue 2 – There was no deletion of transaction data. Coyne has mis-read the Peak.
- Issue 3 – FJ are deleting data from the BRDB but not transaction data.
- Issue 4 - FJ are deleting data from the BRDB but not transaction data.

3.266 → 3.269: PC0241528

Background:

Recovery Data

- Should a failure occur, then (for a recoverable transaction) recovery data will have been stored at the data centre and is the key asset in order to support recovery.
- Recovery data is created during the customer transaction lifecycle at various key points on the counter – with the aim of storing the information required to reconstruct the transaction.
- As documented in DES/APP/HLD/0083[107], page 25, recovery data can exist in different states:
    - **Active** – Recovery data is active and will be returned to the counter should failure occur.
    - **Settlement Completed** – Recovery data is marked as completed by the settlement procedure under non failure conditions.
    - **Recovery completed** – The recovery process has completed and marked the recovery data as complete. The corresponding transaction has been recovered.
    - **Outstanding –** The recovery process was unable to recover this transaction for some reason. To allow the counter to proceed, the recovery data is marked as outstanding and needs to be manually resolved by support staff.
- Recovery data is kept in the 'recovery data table', as per DES/APP/HLD/0083, page 74.
- This Peak relates to a transaction involving recover data being I the 'outstanding' state – i.e. the recovery process was unable to recover the transaction and recovery data is therefore 'marked' as outstanding and needs to be manually resolved by support staff.

Recovery Script

[103] F/1320
[104] F/1220
[105] F/1703
[106] F/611
[107] Disclosed at: POL-0449312 but not in the trial bundle.

FUJ00155196

- Horizon checks to see if any transactions were in progress at the point of the failure (by checking for incomplete transaction records in a 'recovery' transaction table held within the data centre).
- If records are found, Horizon then triggers a Recovery transaction script (note there will be bespoke recovery scripts for each transaction type)
- The purpose of the recovery script is twofold: (i) to make live / online calls to third party systems if required and (ii) to also prompt the clerk for input (e.g. 'was cash payment taken for the transaction before failure'? or 'was a receipt produced?')
- Based on the information received from the clerk and/ or the third party, the recovery script can then complete the original transaction if required, or finish cleanly if no recovery actions are required.
- Once the above is complete, the clerk can then continue with their business.

Dates:

- 3 March 2015 - Raised by FJ following a State 4 report[108]
- 23 March 2015 – issue fixed. No fix to system required, just recovery of the SPM to the correct trading position.

What happened?

- PC0241528[109] relates to a branch with a recovery that was continually failing to complete[110]
- A recovery can be needed in branch where the SPM is experiencing network issues, for example. If the network issues continue, then Horizon can be stuck in the 'recovery loop' where the system is continually failing to recover the transaction, but doesn't display that it has failed.
- The user entered two transactions on a terminal but did not complete them so the basket was not written to the BRDB. They then logged on to another terminal. A user cannot be logged into two terminals simultaneously, so was warned that switching between terminals would cause the transactions on the first terminal to be incomplete.
- The user proceeded anyway. Horizon initiated the recovery process for the two sessions as designed and produced recovery receipts.
- The recovery script however failed and the two transactions were not successfully recovered.
- The 'recovery script' referenced in the Peak is the 'Health Lottery ADCScript" which prevented the user log in. As this script is provided by ATOS, Fujitsu were unable to comment further on what it was or why it would fail, but have confirmed that it is possible this could be a result of the recovery script failing to exit.
- The failure meant that the partial basket became stuck in Horizon. Due to this stuck basket, the user could not log back on. The system basically went into loop of trying to recovery the two transactions and then failing to recover and trying again. It is not possible to log on whilst there is an incomplete recovery task.
- Having investigated the issue, SSC determined that the only way to proceed was to delete the stuck session. The relevant extract from the Peak is below. Node 1 = Counter 1.

```
Date:23-Mar-2015 16:23:29 User:Sudip Sur
[Start of Response]
I have updated the failed session and the PM confirmed that he is now able to
log on Node:1.

[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under
Investigation
Response was delivered to Consumer
```

```
Date:24-Mar-2015 10:21:25 User:_Customer Call_
update from Atos:

Hello Team,
```

FUJ00155196

I have called branch and talk to PM, as per her mention incident got resolved and ready to close the ticket.

Date:**24-Mar-2015 10:28:19** User:**Sudip Sur**
[Start of Response]

MSU please do the necessary reconciliation:

This office was doing a Banking txn 00-145925-1-3891961-1 cash withdrawal txn for £296.70 on 21/2/15 @14:05
The session (1-893961) also contained a non financial Health Lottery txn.

The cash withdrawal txn were authorised and receipt was printed
However PM didn?t settle the txn basket.
While still logged on Node:1, PM then logged on Node:2 at 14:20pm.
User: HP IRRELEVANT was warned about the concurrent login and the session on Node:1 will fail. But the PM carried on login on Node:2. This caused Both txns to fail on Node:1.

On 23/2/15 when the user attempted to logon on Node:1, the recovery kicked-in. But the recovery failed due to Health lottery ADCScript failure and preventing User Logon.

POL Branch Support team have now authorised us to remove/update the session in order for PM to use the node again.
I have carried out and completed the task. PM is now able to use the node again.

Reconciliation needed for the banking transaction:
The cash withdrawal txn was authorised and PM should have paid the money out.
If PM paid the money out as printed on the receipt then customers account should be ok.
However this will leave this office £296.70 short (cash shortage) as the session not completed fully.
POL need to do appropriate reconciliation; transaction correction.

MSU: Please send the call back to me once BIMs have been raised.

- The Peak makes clear that PO authorised this activity as it includes a copy of an email from PO.

From: Anne Allaker
Sent: Friday, March 13, 2015 4:39 PM
To: Post Office Service Desk
Cc: Humphries, Ian; ITSupplierManagement; Patricia Bursi; Ibrahim Kizildag
Subject: RE: Meanwood Post Office- Branch Code2693232 / I6809429

Hi,

FUJ00155196

Yes I did authorise deletion however neither I nor our Network Teams received any confirmation that the session had been deleted.

Pat, in Branch Support Team, however did remain in contact with the postmaster and has confirmed with the branch that the session was deleted and they are able to use the Horizon kit again.

Could you please contact whoever is needed (Fujitsu I presume) and confirm that this is the case please. Alternatively it would be good to know who is responsible for providing confirmation of incident closure.

Thanks
Anne

Anne Allaker
Branch Support Programme

Upper Floors, The Markets Post Office,
6/16 New York Street,
Leeds, LS2 7DZ.
Mobile GRO

- The above extracts do make clear that the branch was communicated with all the way through the process.

'Deleting a session' and recovery marker data

- For completeness: when the system identifies a need for a recovery, there is a record created. It appears in this case that the recovery process didn't run properly which meant that the user couldn't do anything on the counter.
- The Peak does make multiple reference to "*deleting a session*" for this branch and this could easily be read as a lay person as meaning deleting transaction data.
- Having spoken with FJ, we understand that this does not mean deleting the entire user session or basket and its related transaction data. It means deleting an entry from a different database table that is used to record whether a recovery process needs to run or not – i.e. you are deleting the record that says that the transaction needs to be recovered and/ or updating the recovery record to mark the record as having been successfully.
- It is therefore simply deleting this marker/ record rather than the underlying data. Once the marker is deleted, Horizon will no longer be stuck in the recovery loop.

Recovery marker data: relevant documents

- We wanted to point to a document that substantiates the above claim that the relevant data deleted was the recovery marker data and did not include any recovery transaction data – i.e. the data that could be used to recover/ reconstruct the transaction. We have reviewed DES/APP/HLD/0083 (not in trial bundle but disclosed and embedded below) and can see:

FUJ00155196

1. 'Recovery Data' is defined in the table on page 9 as "*Data that is stored to enable a Recoverable Transaction to be completed. Such data must be secured in the Branch database (and the acknowledgement received by the counter) before the transaction is allowed to proceed at the branch.*"
2. The 'Introduction' on page 11 then makes reference to recovery after a failure and confirms that recovery data "*needs to be held in a durable state-store and held at the data centre, in order to reconstruct the transaction*"
3. Recovery Data is held in the data centre in the 'recovery_xml' BRDB Recovery Table field (section Table 1: Recovery Data Storage at 7.2.2.2).
4. As per section 7.2.2.2.1, recovery data can exist in different states. The applicable state in PC0241528/F1320 is 'Outstanding' as this was a recovery that was continually failing to complete. This makes reference to the marker data and confirms "*the recovery data is marked as outstanding and needs to be manually resolved by support staff*".

- To assist Counsel we have prepared the below chronology of what happens (based on DES/APP/HLD/0083):
    1. Before a transaction is completed, details of the transaction are automatically stored in the 'recovery data table' in the data centre, specifically in the recovery_xml table field. This will include the details of the transaction and all appropriate information in order to allow recovery to complete.
    2. Before a transaction is completed, the settlement_complete_timestamp is used to mark recovery as Active (if this field is not completed). This is the 'marker data'.
    3. If the recovery fails and gets marked as Outstanding. Again the 'marker data'.
    4. (outstanding_recovery_item='Y') then the counter can continue and the recovery is effectively skipped and marked for manual intervention. This did not happen in PC0241528/F1320 as the recovery script was not working correctly (DES/APP/HLD/0083 BAL Recovery Data State at 7.2.2.1.)

  As can be seen from the above that the actual recovery data and marker data are held in separate fields but are still held in the same recovery data table.
- There is reference in the Peak to MSC task 'O43T0086557' which should illustrate the steps taken by the SSC team in terms of the options being to update the following fields in the recovery record to mark the session as successfully recovered or delete the record:
    - txn_recovered_timestamp={date recovery complete}
    - outstanding_recovery_item='N'

138009191_native.pdf

Comment for Counsel

- Coyne @ 3.268 comments that the Peak shows a lack of effective communication between PO, FJ and ATOS. This is a fair comment based on this Peak. However, it should be noted that ATOS were appointed in early 2015, so this would have been early in their role.
- Relevant KEL: Surs1034R [F/1318.1]

3.270

- PC0234786[111] is a very short peak.
- Issue raised by SPM call on 11 June 2014. Call closed the same day because an engineer was despatched to the branch.
- A counter terminal broke and needed replacing. The user was logged on at the point when the counter broke. If at the exact moment the counter breaks, a transaction had been added to the stack (but not committed to the BRDB), then a recovery process would be needed to recover that transaction.
- This situation is localised to a single basket of transactions that were in process when a terminal becomes irreparably broken.

[111] F/1220

FUJ00155196

- Coyne says that this is similar to the above issue.
    - It is not the same. The above related to a failed recovery script. This issue is to do with a broken counter. They are completely different.
    - Also, he says that this Peak relates "to a failed session requiring Fujitsu to perform deletion of session data". That is not what the Peak says – extract below. The SSC was not saying that a deletion WAS required but that a deletion MAY be required.
    - The fact that the Peak was closed with no further comments is good evidence that no deletion was required – compare this to the level of commentary included in the Peak above where a deletion did happen. It is likely (but there is no written evidence to support this) that the on-site engineer was able to get the terminal working and the recovery process ran automatically to correct any issues.

```
Date:11-Jun-2014 15:07:42 User:Sudip Sur
[Start of Response]
Please wait until engineer installed the node again and the session recovered
by the system.
If this is so urgent then a higher priority TFS call should be raised to get
Romec engineers out to site.

We do not know what transaction PM was doing in the failed session. Therefore
If NBSC still wants us to remove this session then they have to formally
authorise us to remove this session as we do not wish to be held responsible
for any transaction losses which may cause financial discrepancy during
rollover.
```

3.271 → 3.274 : PC0263716 F/1703

Dates:

- Issue raised by SPM on 26/10/17
- Solution identified the same day .
- Solution implemented on 2 Jan 2018 (the first attempt to solve the issue failed)

What happened?

- PC0263716[112] is a very long and messy peak.
- A counter was migrated from HNG-X to HNG-A (both version of Horizon Online, but running on different versions of Windows) by physically swapping the terminal.
- Fujitsu have confirmed that the migration was irrelevant, as the issue was caused by the downsizing of the office from 2 counters to 1, although potentially this could have happened at the same time as the migration.
- A user was logged on to the counter 2 and did not properly log off before the counter was removed. This is recorded as a failed session because the user cannot log out and Horizon thinks they are still logged in and is the cause of the issue here.
- Because the user was attached to a stock unit, the stock unit could not be released from the user and the stock unit could not be rolled over.
- The solution was to delete the session associated with the logged in user. Relevant extract from the Peak below:

```
From: Gillian Hoyland
Sent: Wednesday, November 22, 2017 11:18 PM
To: Post Office Service Desk
Cc: Paul I Smith
```

FUJ00155196

Subject: RE: ATF:I7186625 | Session Correction Request

Hi

Due to the circumstances at the branch this session can be removed but the branch must be made aware that if there are any losses/gains from removing it then they will be liable.

Please note, in future any requests of this nature that do not have the applicable form attached which shows what the transaction was for, date etc will not be actioned by FSC until this form is received as this allows us to investigate the incident.

Thanks
Gill

Gillian Hoyland
FSC Operational Support Manager

Date:**20-Dec-2017 13:47:45** User:**Joe Harrison**
To resolve this I need to run the following SQL on a BRDB instance

```
delete from brdb_branch_user_sessions
where branch_accounting_code = 111832
and fad_hash = 124
and node_id = 2
and session_status = 'FAILED' or session_status = 'RECOVERING'
```

PLease can you authorise the unix team to grant me the "set role appsup" permission.

Date:**20-Dec-2017 13:48:32** User:**Joe Harrison**
The Call record has been transferred to the team: Security Ops
Progress was delivered to Consumer

Date:**22-Dec-2017 10:28:30** User:**Joe Harrison**
Operation complete - please transfer call back to me for closure.

Date:**27-Dec-2017 14:35:15** User:**Joe Harrison**
[Start of Response]
The failed transaction has been deleted so please inform the branch that they should now be able to rollover. We will supply formal closure later.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Response was delivered to Consumer

- Note – Paul Smith is copied to the top email and he is a witness.
- The above solution failed because further data needed to be deleted. FJ also needed to delete the recovery transactions.

Date:**02-Jan-2018 14:23:48** User:**Joe Harrison**
KEL surs3213P warns: "Any unsettled entries in the Recovery table may also

FUJ00155196

need to be cleared (so far this has not been required)."

We think in this case it is in fact required. We propose to run the following SQL on BRDB 3

delete from brdb_rx_recovery_transactions where BRANCH_CODE = '111832' and FAD_HASH = '124' and NODE_ID = '2'

Can I have "role appsup" again please

Date:**02-Jan-2018 14:24:41** User:**Joe Harrison**
The Call record has been transferred to the team: Security Ops
Progress was delivered to Consumer

Date:**02-Jan-2018 15:55:49** User:**Joe Harrison**
The SQL used was actually

delete from ops$brdb.brdb_rx_recovery_transactions where BRANCH_CODE = '111832' and FAD_HASH = '124' and NODE_ID = '2'

Date:**02-Jan-2018 16:01:58** User:**Niall Vincent**
The Call record has been transferred to the team: EDSC
Progress was delivered to Consumer

Date:**02-Jan-2018 16:14:56** User:**Daniel Best**
The Call record has been assigned to the Team Member: Joe Harrison
Progress was delivered to Consumer

Date:**02-Jan-2018 16:18:50** User:**Joe Harrison**
[Start of Response]
I deleted the recovery transaction which the KEL says has never previously been necessary to fix a session stuck in a lost counter. Maybe it is needed now for some reason. Please ask PM to try rollover again.
[End of Response]
Response code to call type L as Category 67 -- Final -- Solicited Known Error
Routing to Call Logger following Final Progress update.
Service Response was delivered to Consumer

Date:**02-Jan-2018 16:18:50** User:**Joe Harrison**
CALL PC0263716 closed: Category 67 Type L

Comments for Counsel

- Having spoken to FJ we understand that the above is not a reference to deleting transaction data. Two things have happened:
    - Deletion of a session marker, because the marker was showing the session as "failed" or "recovering". This deletion was made in the BDRB but to the table: brdb_branch_user_sessions. This is not a table holding transaction information. This is all shown in the Peak extract below that describes the deletion of the session (marker) that was still open on the removed Counter 2:

FUJ00155196

Date:**20-Dec-2017 13:47:45** User:**Joe Harrison**
To resolve this I need to run the following SQL on a BRDB instance

```
delete from brdb_branch_user_sessions
where branch_accounting_code = 111832
and fad_hash = 124
and node_id = 2
and session_status = 'FAILED' or session_status = 'RECOVERING'
```

PLease can you authorise the unix team to grant me the "set role appsup" permission.

- Deletion of a recovery session for the same reasons as above. Again this is just deleting the marker that a recovery is required, not the actual transaction data. This is also shown in the Peak.
- Note, this is also an example of 'recovery data' being deleted, see above comments on 3.266 → 3.269: PC0241528, Background: Recovery Data section.

Date:**02-Jan-2018 14:23:48** User:**Joe Harrison**
KEL surs3213P warns: "Any unsettled entries in the Recovery table may also need to be cleared (so far this has not been required)."

We think in this case it is in fact required. We propose to run the following SQL on BRDB 3

```
delete from brdb_rx_recovery_transactions where BRANCH_CODE = '111832' and
FAD_HASH = '124' and NODE_ID = '2'
```

Can I have "role appsup" again please

- Note that entry in the Peak, extract below, incorrectly refers to the data as a "failed transaction", when this should be the session data relating to the failed transaction:

Date:**27-Dec-2017 14:35:15** User:**Joe Harrison**
[Start of Response]
The failed transaction has been deleted so please inform the branch that they should now be able to rollover. We will supply formal closure later.

- The Peak contains extracts from emails that make clear that PO authorised the deletion. FJ were rigorous in obtaining authorisation before doing anything.

From: MAC
Sent: 26 October 2017 14:41
To: Post Office Service Desk <PostOfficeServiceDesk GRO >
Cc: MAC <[redacted] GRO >
Subject: A17004602/I7186625

Hi

Please see below update from our software team and raise this with POL for authorisation to remove the failed session:

FUJ00155196

Session 994149 sequence number 5036725 has an empty SETTLEMENT_COMPLETE_TIMESTAMP therefore I believe this is an instance of KEL surs3213P and the following response is the one instructed in that KEL.

Branch 111832 cannot roll over stock unit AA, or the office, because of a failed user session on node 2, which was removed on 23/10/2017. The last user, JS IRRELEVANT did not log out cleanly.

If node 2 has been permanently removed and cannot be temporarily reinstated, the failed user session will have to be deleted from the database without the opportunity for the normal recovery process to run. This can be done by Fujitsu but requires formal approval from Post Office.

If there was an uncompleted customer session (basket) when the counter was removed, this might lead to a financial discrepancy. We cannot tell whether there was such a customer session, and Fujitsu Services will not accept responsibility for any potential financial discrepancy as a result of deleting the user session.

Regards
Emma Millman

- The Peaks makes clear that this has happened before:

  From: MAC
  Sent: 26 October 2017 17:48
  To: Post Office Service Desk <PostOfficeServiceDesk GRO
  Cc: MAC < GRO >
  Subject: RE: A17004602 - I7186625

  Hi

  What is the next course of action then?

  POL have previously authorised removal of a session that is not related to travel money card plenty of times in the past.

  Regards
  Emma Millman

FUJ00155196

- Also, that there appears to be a process for this and a form to be completed.

2017-10-26 11:39:37 [Watts, James Marcus]
HDIoutSTU : From: Post Office Service Desk
[mailto:PostOfficeServiceDesk GRO
Sent: 26 October 2017 12:36
To: MAC <GRO
Subject: RE: A17004602 - I7186625

Hi Jackie,

Apologies for this late response.
We already sent to POL the session correction form and just awaiting for their approval.
We'll let you know as soon as we have receive a response.
Please see below are the HNG-A versions for this branch .

Session data: relevant documents

- We wanted to point to a document that confirms (1) what session marker data is and (2) where session marker data is stored.
- PC0263716 F/1703/25 confirms that session marker data is stored in the brdb_branch_user_sessions table.
- In terms of showing that the session marker data is stored separately to details of the actual session/ transaction data, there is no document that explicitly states it but this can be inferred from the following sections of DEV/APP/SPG/0017[113] (embedded below):
    - Section 6.9.1.4.2 User Tables: BRDB_BRANCH_USER_SESSIONS "*Holds all session information for a user. Entries in this table are created at login and updated during the authentication process. This table is used as a cache for SRP information during authentication.*"
    - Section 4.2.1.2.5 Accounting Database Tables which shows that the BRDB_RX_REP_SESSION_DATA is held in the Accounting Database tables, which is separate to the session data referred to in PC0263716

  If counsel sees the benefit, one option here could be to obtain a witness statement from one of the design team at FJ to confirm the above, as we understand it is not documented in any other Design Document (to the best of FJ's knowledge).

DEV/APP/SPG/0017:

138039458_native.pdf

[113] Not in the trial bundle but disclosed at POL-0108180

FUJ00155196

3.275 → 3.276

- This incident[114] occurred on 12 April 2010, shortly after the affected branch was migrated to Horizon Online.
- During the migration certain data was added to database table (not the one for transaction data) to assist with the migration.
- This created a bug that prevented some branches from rolling over into a new trading period.
    - There was no loss of transaction data or financial impact on the branches.
    - The branches were still able to trade like normal.
    - They just could not complete the last step in their end of month accounts ie. rollover and move to another trading period.
- The solution was to delete the problem data from the database. The data is not transaction data and Coyne acknowledges this in para 3.276, although branch data affecting the branch's accounts, being a false opening balance for the next trading period, was deleted.
- This is a short Peak[115]. Relevant extract below.

Date:**14-Apr-2010 11:42:56** User:**Anne Chambers**
[Start of Response]
On BRDB, BRDB_BRANCH_INFO says they are in TP 11 and last rollover date is 17th Feb. BRDB_BRANCH_STOCK_UNITS says DEF is TP 12.

I've retrieved logs of an attempt to roll the office from TP 11 to 12, at 9:51 UTC 12th April.

All looks ok - trading statement is printed, and they press confirm. Message with requestid 314642-3-K2-1209-123 jsn 5326045 is sent to RolloverBranchService. This times out at the counter.

The bal osr log shows an exception while executing statement insertOpeningBalanceForRollover - OPS$BRDB.BSOB_PK violated.

I suspect this may be because there is already a single entry in BRDB_SU_OPENING_BALANCE for DEF TP 12 BP 1, inserted during migration. The entry is for cash, zero value.

I'm wondering if this branch could be sorted out by changing the TP in BRDB_BRANCH_INFO (this would have to be done by OCP by development/ISD). The PM already has several printed copies of the TP 11 BTS. From the logs, I can see that suspence and cash/currencies awaiting collection are all zero - so no office opening figures are required for TP 12??

This needs looking at urgently for a workround for this branch, and longer term to see if this can be avoided at other migrating branches.
[End of Response]
Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Response was delivered to Consumer

Date:**14-Apr-2010 11:43:29** User:**Anne Chambers**
Evidence **Added** - Obfuscated logs

Date:**14-Apr-2010 11:44:03** User:**Anne Chambers**
The Call record has been transferred to the team: Bus_Apps_Des
Progress was delivered to Consumer

Date:**14-Apr-2010 13:00:09** User:**Gareth Jenkins**
[Start of Response]

FUJ00155196

```
I?ve had a look at this Peak and agree that we need an OCP to tidy up BRDB to
?un-stick? this Branch. Note that what I am proposing here is slightly
different from what Anne has suggested above.

What we need to do is the following:

(I know the SQL is wrong, but BRDB Host team can correct it and fill in the
gaps.)

1. Update BRDB_BRANCH_STOCK_UNITS WHERE fad_hash = ??? AND
Branch_accounting_code = 314642 AND stock_Unit = ?DEF? setting trading_period
to 11

2. Delete BRDB_SU_OPENING_FIGURES WHERE fad_hash = ??? AND
Branch_accounting_code = 314642 AND stock_Unit = ?DEF? trading_period = 12
(Anne asserts that there is one such row with zero value for prod_id = 1. I
suggest that this is checked by doing a SELECT first.

What this will do is re-align SU DEF?s TP with that of the Branch. It should
then be OK to rollover the Branch again.

BRDB Host will fix this by OCP.

It is accepted that this will probably re-occur during Migration. However it
is proposed that we wait for Branches to report the issue and fix via OCP (in
a similar way to this one). Also need a KEL.
[End of Response]
Response code to call type L as Category 94 -- Final -- Advice and guidance
given
Routing to Call Logger following Final Progress update.
Response was delivered to Consumer
Defect cause updated to 7 -- Design - High Level Design
```

Comments for Counsel

- Coyne's summary is fair on this but irrelevant to his case on PO deleting transaction data.
- Relevant KEL: acha4942M (not currently in trial bundle but in bundle of additional KELs)

FUJ00155196

SECTION 4: PEAKS WITH EVIDENCE OF REMOTE ACCESS: PARAS 3.277 – 3.287

- Coyne deals with a number of 'Peaks' with evidence of Remote Access in this section;
- Coyne addresses 2 issues:
  - Para 3.277 - PC0208119[116] and the use of APPSUP; and
  - Para 3.283 - Policy adherence in the context of the deletion of data from the Branch Database.

3.277: APPSUP

- This issue concerns the APPSUP role. Coyne attempts to make two points about this role, without expressly saying either:
  - APPSUP is something new that PO have not disclosed before.
  - APPSUP is used only for emergency access and that has happened 2,000+ times which suggests something is wrong.
- APPSUP is the more accurate term for a certain type of privileged user access within the BRDB.
  - It is not a special tool or new way to change transaction data.
  - Within the access permission structures for any database, a number of pre-designed roles are created. Each role comes with a different bundle of rights and powers. A role can be assigned to different users at different times and multiple users can have the same role.
- Within SSC staff, the default level of access to the BRDB is effectively "read only" and "execute", the latter meaning that SSC can execute pre-written scripts and tools, which may in effect change the BRDB and transaction data. SSC users cannot directly edit transaction data with this level of access.
  - APPSUP is the name of the designated role for a user that has a higher level of privileges.
  - With this level of access, it is theoretically possible to amend transaction data stored in the BRDB.
  - Note – APPSUP is specific to the BRDB only, but similar roles with other names will almost certainly exist in other databases within Horizon.
- Peak PC0208119 cited by Coyne is discussing the circumstances in which SSC personnel may need the APPSUP role.
  - A bug had arisen that needed a fix applying to the Horizon software. 4th line development had asked SSC to do this. To do this, SSC staff needed to have the SSC role. However, SSC staff only have read only access but did have the ability to switch to the APPSUP role.
  - As per the Peak (30 September 2011 14:20 entry at F/768/3), while the SSC should have access to it they should only be given the optional role 'temporarily'.
  - The Peak discusses the nature of the role that SSC should have going forward.
  - It is decided that SSC should have the SSC role, and have the power, in emergencies, to be given the APPSUP role.
  - The Peak is not discussing the amendment of any transaction data; it is talking about amendments to the BRDB software and configuration.
- The key section of Coyne's commentary is at para:

3.279 Coyne 2: 'Appsup' is described briefly in the same PEAK (also including a warning) by Andy Beardmore in 2011:

- *"The optional role 'APPSUP' is extremely powerful. The original BRDB design was that 3rd line support should be given the 'SSC' role (which is select_any_table + select_catalogue) and only given the optional role 'APPSUP' temporarily (by Security Ops authorisation) if required to make emergency amendments in BRDB Live. Since then Host-Dev have delivered a series of auditable amendment tools for known SSC data amendment operations in Live, and these are assigned by role to individual SSC user accounts. As such SSC should not require the APPSUP role in BRDB, unless there is an unforeseen update required to Live. Transferring to Steve Parker for review/assessment… It is a security breach if any user write access is not audited on Branch Database, hence the emergency MSC for any APPSUP role activity must have session*

[116] F/768

FUJ00155196

logs attached under the MSC. Host-Dev previously provided scripts, such as the Transaction Correction Tool, are written to run under the SSC role and also write to the audit logs."

3.280 I understand Mr Beardmore to be explaining that APPSUP should not be used to access the branch database. It was only designed for emergency amendments to the live branch database but acknowledging that such action whilst logged is not audited, Mr Beardmore advises that "auditable amendment tools" are available to SSC.

Coyne's understanding

- Coyne's understanding is not quite right.
    - The SSC has its own designated role (the SSC role) and a series of tools built to help it do its job – including the Transaction Correction Tool (ie. Balancing Transactions).
    - This does not mean that other users may make use of the APPSUP role outside of SSC for ordinary work on the BRDB.
    - This is readily apparent if one reads the whole Peak.
- Coyne goes on to look at the privileged user logs and notes that APPSUP access has been used 2000+ times. He therefore assumes that there has been 2,000 emergency corrections to the database.
- This is an incorrect conclusion once one realises that APPSUP is used by some users outside SSC for non-emergency maintenance[117] (explained below).

Analysis of APPSUP logs

- Fujitsu have examined the APPSUP logs which record that the APPSUP role was used 2,175 times between 2009 and 2018 and confirm they have found:
    - 94 represent declined APPSUP requests.
    - 1,730 represent scripted support work requested by Post Office (Fujitsu have confirmed this would have no financial impact to SPM accounts). Note this is the non-emergency maintenance we previously referred to as 'ordinary database maintenance'.

  This leaves 351 audit entries for APPSUP used over the 2009 – 2018 period (21.12.2009 – 05.06.2018).
- Fujitsu have additionally confirmed that the APPSUP logs show all 'usage' of the privilege/ role and confirmed that when a technician is using APPSUP they will not usually execute a single action. As such, there could be several logs/ entries relating to the same session, for example, all of the following steps undertaken by the user could be recorded as a separate entry:
    - Gain the required privilege
    - Use commands to examine information
    - Use a series of commands to complete the support action
    - Use commands to examine the revised information to check that the action has been effective
    - Relinquish the required privilege

  All of the above steps would be audited as a separate 'use' of APPSUP/ entry in the log, meaning the 351 figure is likely to higher than the true number of sessions the APPSUP role relates to.
- In relation to determining how many separate support sessions of the APPSUP role the 351 truly represents, Fujitsu have performed a further analysis and defined a 'support session' as encompassing all APPSUP audit entries for the same user within a one hour period.[118] Using this criteria, Fujitsu have estimated that the APPSUP privilege (outside of the declined and scripted support work) was actually used in 284 support sessions as follows:

[117] Note for counsel: note the change here from ordinary database maintenance to non-emergency maintenance.
[118] Note for counsel: we have not asked Fujitsu why this classification was made by presume it is because most sessions/ tasks using APPSUP are likely to take approximately one hour.

FUJ00155196

Year	Sessions
2009	1
2010	78
2011	37
2012	24
2013	16
2014	26
2015	27
2016	45
2017	23
2018	7
Total	**284**

Note, we have not requested detail in the logs from Fujitsu to evidence the above at this stage.

Conclusion

- This 284 figure across the 101 month period equates to an average of less than 3 uses per month and appears to be more consistent with these "*unforeseen updates*" required to Live, as described in the Peak, and alone confirms that privileged access by Fujitsu is not excessive.
- In terms of analysing these 284 sessions/ uses of APPSUP, the only way to thoroughly do this would be to review each of the Peaks to ascertain what action was undertaken.
- Fujitsu have performed an initial analysis that indicates that there may have been three other categories of usage here:
    - Erroneous recovery scripts
      (estimated at 50 sessions)
    - Failed user sessions
      (estimated at 105 sessions)
    - Migration
      (estimated at 79 one-off actions during migration to move branches from Legacy Horizon to Horizon Online)

  The above is approximate but would leave 50 remaining support sessions, again strengthening the position that use of APPSUP was not excessive.

- **Notes for Counsel**

- The full peak makes clear that SSC users used to have access to elevate privileges to APPSUP for 'write' (as opposed to read-only) access to the database.
- One line of attack that Green may pursue against Fujitsu is that there is no record of what was done when the privileges were elevated and furthermore Fujitsu could choose to switch roles without seeking prior approval.
- Fujitsu have confirmed they have always (and will always) need the ability to write to the databases, following whatever change control process is currently in place. Whether this is via APPSUP or SSC roles is completely irrelevant as Fujitsu's requirements are the same either way. Fujitsu's view is that this was not a poor security practice as the switching of roles is audited. It therefore more comes down to the issue of the lack of approval required.

FUJ00155196

- **Coyne (3.278)** quotes Anne Chambers' comment in the Peak: "*When we go offpiste we use appsup*". Coyne appears to be seeking to indicate some sort of improper use of the function here. Fujitsu have confirmed this comment refers to the use of APPSUP to resolve an issue where there is no set process in place. This therefore aligns with the update in the same Peak by Andy Beardmore which Coyne quotes at para **3.279** in that the APPSUP functionality/ tool is used where circumstances require an unforeseen update to be made to Branch Database live.
- **Coyne** (**3.280**) states that the APPSUP function was logged but not audited. Mr Coyne has had sight of those logs and indeed at para 3.281 confirmed his review of the privileged user access logs which document the use of the APPSUP function. Note these logs have been disclosed but are not in the trial bundle.
- Finally, we originally made reference to APPSUP being used for 'ordinary database maintenance'. This was a point we discussed in detail during a call with Fujitsu who confirmed that APPSUP was not used for this purpose. It is acknowledged that the 1,730 uses of APPSUP relating to the scripted support work requested by Post Office did arguably amount to 'routine' maintenance due to the volume of times the role was used. Having discussed this with Fujitsu in further detail, we understand that this is work that Fujitsu could have charged an additional cost to Post Office for doing but they didn't. Note, there is nothing in the Peak to confirm that APPSUP was also used for this purpose/ in this way by Fujitsu.

3.283: Policy Adherence

This section does not refer to a live issue or new form of remote access. It relates to general comments about FJ adherence to internal policy. FJ's comments on this are embedded below.

3.283_Policy Adherence.docx