WITN09880100

Witness Name: Jonathan Richard Hulme

Statement No.: WITN09880100

Dated: 16 August 2023

POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF JONATHAN RICHARD HULME

I, *MR JONATHAN RICHARD HULME*, will say as follows:

INTRODUCTION

1. I am currently employed by Fujitsu Services Limited ("**Fujitsu**") as a Solution Architect on Fujitsu's Post Office Account, with a particular focus on the Horizon counter application.

2. This witness statement is made to assist the Post Office Horizon IT Inquiry (the "**Inquiry**") with the matters put to Fujitsu in Rule 9 Requests dated 16 June 2023 and 31 July 2023 (the "**Requests**"), to the extent I have or had direct knowledge of such matters. Where I have referred to documents to assist my preparation of responses to the Requests, the URNs of the relevant documents are set out in this statement.

3. I was assisted in preparing this statement by Morrison Foerster, the recognised legal representatives for Fujitsu in the Inquiry.

WITN09880100

PROFESSIONAL BACKGROUND

4. I graduated from Southampton University in 1983 with a first-class Joint Honours Bachelor of Science degree in Physics with Computer Science and joined ICL (later Fujitsu) in October 1983. I have held various roles within the company as a software developer, then software designer, and later a solution architect.

5. I worked briefly on Legacy Horizon as a counter developer from June 2004 to October 2005 and have very little recollection of Legacy Horizon. I have worked on the development of the Horizon Online ("**HNG-X**") counter since November 2007 which was later rolled out in 2010.

6. In light of the above, my responses to the questions in the Inquiry's Requests are focused on my knowledge of HNG-X only. This statement sets out a summary of the complex technical position relating to the Inquiry's Requests as I now recall and understand it. Although I have referred to documents in preparing this statement, in the time available, I have not reviewed every relevant technical document. Accordingly, there may be technical details or exceptions that I have misremembered or forgotten.

7. Given that the questions asked by the Inquiry relate to the behaviour of complex software, my responses in this statement describe what the software was designed to do. There is always the potential for defects to be present which might mean the software does not behave as it was designed. To the extent that I recall such defects, these are described in this statement. However, the defects in this

WITN09880100

statement are indicative only and are not intended to be an exhaustive list of all relevant known defects.

SIMULTANEOUS LOG-INS

8. The Inquiry has asked Fujitsu to explain whether it is possible for a postmaster or "user" to be logged on to more than one node (or "counter") simultaneously, using the same User ID. This is not a straightforward question, as the relevant functionality has changed over time.

9. In the context of HNG-X, simultaneous logon behaviour was specified by the use case entitled 'BAD-11 Log On to system v5.06 20110830' dated on or around 30 August 2011 (the "**Initial Log On Use Case**", FUJ00171897), notably (i) variation BAD-3599 "*Concurrent Log-on: Active Session Successfully Terminated*", which can be identified from the left hand column of the Initial Log On Use Case, and (ii) business rule BRU-701.

10. At this time, business rule BRU-701 stated that "*[a] User shall only be able to be logged on to one Counter or Terminal (in a branch) at any one time*" (see the document entitled '_Design_Authority_Business_Rules_v5.09_20111207', FUJ00171898, and dated on or around 7 December 2011 in this regard).

11. By way of background for the Inquiry, use cases provide a user-centric specification of counter behaviour, and business rules state low-level business requirements for the counter behaviour – these were written when HNG-X was ported from Legacy Horizon, and were owned and maintained in Post Office Limited's ("**POL**") Requirements system, "DOORS". POL subsequently

WITN09880100

decommissioned their "DOORS" system and ceased maintaining counter use cases and business rules, so Fujitsu took on maintaining the use cases and business rules as Word documents and Excel spreadsheets on behalf of POL.

12. During the time these use cases were in place, for example, if a user logged on to a second node, the system would identify if they were already logged on to a first node. At this point, the second node displays message "MSG04002" and the user could then choose to:

12.1 Continue logging on to the second node; or

12.2 Cancel logging on to the second node.

13. In the first scenario, where the user continued logging on to the second node, the system marked the first node's user session as having failed, but would only force the first node to logout when that node next talked to the data centre. At least in a development environment, not every type of interaction with the data centre causes that node to force logout, although the exact details of this are outside my area of knowledge.

14. A user can also lock the counter node, and then has to enter their logon credentials to unlock the node (see variation BAD-3162 "*Log on after Temporary Lock*", in the Initial Log On Use Case). At this lock screen, another user can enter their user logon details to logout the original user's session on that node and return the node to the logon screen (see variation BAD-3217 "*Log off by a new user after temporary lock- confirmed*" and subsequent sections in the Initial Log On Use Case).

WITN09880100

15. The position became more complicated following the introduction of changes regarding Smart IDs / End User Management ("**EUM**"). See the document entitled 'CP6701Att1' and dated 12 December 2017 (FUJ00171899), which describes changes impacting concurrent logon.

16. I am not the subject matter expert for the EUM changes, but I am aware of the following:

16.1 A change to HNG-X was made through EUM to introduce "smart users". Following the introduction of this functionality, multiple Horizon user IDs (HUID) could be linked to a Post Office user Identifier ("**POID**").

16.2 BRU-701 was changed to say "*[a] User shall only be able to be logged on to one Counter or Terminal (in a branch) at any one time. Where a <username> is linked to a <Post Office Identifier>, then the User shall only be able to be logged on to one Counter or Terminal (acrossall branches) at any one time.*" See the updated use case entitled 'BAD-11 Logon to system v5.06 20221215' and dated 15 December 2022 in this regard ("**Updated Log On Use Case**", FUJ00171900)

16.3 A user linked to a POID can logon to more than one counter at once if their other session(s) are locked - see the Updated Log On Use Case (in particular variation BAD-3599) and updated business rules entitled 'Business Rules FJ 20230215' and dated 15 February 2023 (in particular BRU-701, BRU-CP2368-1, BRU-CP2368-2) (FUJ00171901).

WITN09880100

16.4 There were some issues / defects with the EUM changes, primarily around (i) stock unit and branch balancing locking, and (ii) attaching a user to a stock unit while still logged in to another locked node. I became involved with these issues at the relevant time and wrote document 'CP6925 Att2', dated 10 January 2019 (FUJ00171905) to address them. This change was subsequently implemented and released. In particular, I note that:

16.4.1 Section 1 of CP6925 Att2 lists two Peaks recording incidents that occurred in the live estate and which triggered this Change Proposal (see PC0275532 raised on 27 November 2018 and PC0275564 raised on 28 November 2018, FUJ00171906 and FUJ00171918 respectively); and

16.4.2 Section 6.1.1 lists defects which were identified during the investigation and design phase. In addition to the Peaks listed in this section (copies of which are exhibited to this statement, see FUJ00171920, FUJ00171923, FUJ00171924, FUJ00171927, FUJ00171931 and FUJ00171932). I also assisted in investigating defect PC0279931 during September 2019 (FUJ00171933) which regarded a user being unable to logon due to issues checking Horizon user IDs and Post Office user IDs.

17. When a user logs on or off from the system, information is recorded in the counter log of the impacted counter, but these logs only exist for a number of days and are not centrally recorded. A "reporting event" is also generated which is recorded in

WITN09880100

the branch database. See the events listed in version 7 of the document entitled 'HNG-X COUNTER AUDIT EVENT IDS' (DES/APP/HLD/2255) dated 18 May 2022 (FUJ00171938).

18. For the scenario where a user logs on to a second counter node when already logged onto a first counter node, the following events are generated.

19. For the second node:

19.1 EventID 119 is written by data centre, which states "*Concurrent login detected for User <User Id>. Awaiting user response to continue or cancel.*"

19.2 If the user presses "continue" on the warning message (MSG04045 is used instead of MSG04002 for a POID user) then the following two events are written by the data centre for the second node (no matter whether the user was a POID user or not):

19.2.1 A second EventID 119, which states "*Existing session for User <UserId> in Branch <BranchId> at Counter <NodeId> marked as failed.*"

19.2.2 EventID 12, which states "*User <User Id> logged on*".

20. When the first counter node then interacts with the data centre and is told its session has failed, it logs off offline. No event is recorded by this node for the offline logoff.

WITN09880100

TIMESTAMPS IN THE AUDIT DATA

21. The Inquiry has asked Fujitsu to explain how timestamps areset or recorded in the "logfile" and synchronised across branch counter nodes. It is not clear from the Requests which log file the Inquiry intends to refer to. I therefore address below my understanding of log files in HNG-X in relation to which I have a degree of direct knowledge:

    21.1 Counter log file entries record the date/time using the local counter clock.

    21.2 The event date/time on events generated by the counter clock. Event 12 (Logon completed), 101 (Failed Logon), and 119 (concurrent logon) are generated by the Online Service Router ("**OSR**") running on the Branch Access Layer ("**BAL**") platform in the data centre, but use the time of the request sent by the counter which again uses the counter clock (but see PC0280046 raised on 12 September 2019, FUJ00171943).

    21.3 I understand that the clocks on counters and in the data centre are synchronised via a network time protocol, but I do not have direct knowledge of this.

22. I recall assisting with the investigation of defect PC0279931 (in September 2019) (FUJ00171933) which regarded a user being unable to logon due to issues checking Horizon user IDs and Post Office user IDs. A secondary issue found during the investigation was that the counter clock had drifted 34 seconds from the data centre BAL clock. This was raised as PC0280046 on 12 September 2019 (FUJ00171943). The clock drift made it difficult to compare event times, because

WITN09880100

prior to this defect the time of OSR events was generated using the BAL clock. As a result of this Peak, the OSR was changed to use the counter message request time sent so that all the events relating to a counter logon would use that counter's clock.

23. The issue of the clock drift was raised as PC0280437 on 3 October 2019 (FUJ00171944), which was handled by the Software Support Centre.

24. I am also aware that there was a major incident a few months ago where a time synchronisation server reset itself back a number of years. This had a knock-on impact on audit. I was part of the team tasked with investigating the issue. Exhibited to this statement at FUJ00171946 is a copy of the paper prepared as a result of those investigations.

OFFLINE TRANSACTIONS

25. The Inquiry has asked what the expected reporting would be in the "log files" when transactions have taken place offline. However, in relation to HNG-X, it is not possible to transact offline.

26. If a user tries to settle a basket offline, the counter waits for the response from the data centre for 30 seconds and on time-out performs one automatic retry. If that also times out, then the user can perform further retries or alternatively cancel the settlement. On cancellation, the disconnected session receipts are printed, and the user is then automatically logged-off.

WITN09880100

27. In terms of how this would be recorded:

27.1 The counter logs would show the basket being sent to the data centre, but no response received;

27.2 The OSR logs would show whether the message was received and a response issued by the data centre;

27.3 The Branch Database would record the basket only if the settlement message was received; and

27.4 If the counter is automatically logged off due to time-out then it is logged off offline (since it cannot talk to the data centre) and so no logoff event is recorded.

28. The counter will enter Recovery at next logon and, if needed, take the appropriate action to bring the data centre back in line with the disconnected session receipt.

29. When the counter logs back on, the logon completed event (12) is recorded, and if recovery runs then one of the following events is recorded by the counter:

29.1 111: Recovery Completed;

29.2 112: Recovery Completed with exceptions;

29.3 118: No recovery required; or

29.4 120: Recovery Failed.

WITN09880100

ARQ DATA

30. In addition to the matters addressed above, the Inquiry has also asked a number of follow up questions relating to the reliability and sufficiency of ARQ data provided by Fujitsu to POL. Given my roles as a software developer, software designer, and later a solution architect, I do not have direct knowledge of the content of ARQ data or of any specific instances of when this data may have been provided to POL. I am not therefore in a position to comment on the sufficiency of the ARQ data provided over time.

31. In relation to the reliability of the audit archive from which ARQ data was extracted, other than those issues outlined in this statement above, I do not recall any further issues that may have impacted the audit archive. That being said, given that I am not a subject matter expert in this area, I would not necessarily expect to have been made aware of any issues in this part of the Horizon system.

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated: 16 August 2023

WITN09880100

INDEX TO FIRST WITNESS STATEMENT OF JONATHAN RICHARD HULME

Exhibit No.	Description	Control Number	URN
1.	Document entitled 'BAD-11 Log On to system v5.06 20110830'	POINQ0178078F	FUJ00171897
2.	Document entitled '_Design_Authority_Business_Rules_v5.09_20111207'	POINQ0178079F	FUJ00171898
3.	Document entitled 'CP6701Att1'	POINQ0178080F	FUJ00171899
4.	Document entitled 'BAD-11 Logon to system v5.06 20221215'	POINQ0178081F	FUJ00171900
5.	Document entitled 'Business Rules FJ 20230215'	POINQ0178082F	FUJ00171901
6.	Document entitled 'CP6925 Att2'	POINQ0178086F	FUJ00171905
7.	Peak PC0275532	POINQ0178087F	FUJ00171906
8.	Peak PC0275564	POINQ0178099F	FUJ00171918
9.	Peak PC0276050	POINQ0178101F	FUJ00171920
10.	Peak PC0275906	POINQ0178104F	FUJ00171923
11.	Peak PC0275902	POINQ0178105F	FUJ00171924
12.	Peak PC0275893	POINQ0178108F	FUJ00171927
13.	Peak PC0275890	POINQ0178112F	FUJ00171931
14.	Peak PC0275644	POINQ0178113F	FUJ00171932
15.	Peak PC0279931	POINQ0178114F	FUJ00171933
16.	Document entitled 'HNG-X COUNTER AUDIT EVENT IDS' (DES/APP/HLD/2255)	POINQ0178119F	FUJ00171938
17.	Peak PC0280046	POINQ0178124F	FUJ00171943
18.	Peak PC0280437	POINQ0178125F	FUJ00171944
19.	Post Incident Report: IRE19 Galleon Time Server Issue 27 03 2023 (SVM/SDM/INR/4831) v0.4 dated 5 April 2023	POINQ0178127F	FUJ00171946