WITN04830100

Witness Name: Simon Andrew James Fawkes

Statement No.: WITN0483_01

Exhibits: WITN0483_01/1 – WITN0483_01/4

Dated: 9 August 2022

POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF *SIMON ANDREW JAMES FAWKES*

I, *MR SIMON ANDREW JAMES FAWKES*, will say as follows:

INTRODUCTION

1. I am currently a Principal Solutions Architect at Fujitsu Services Limited ("**Fujitsu**"), working on a large government infrastructure outsourcing contract, a position I have held since around 2006. I was designated as a Fujitsu Distinguished Engineer in 2013.
2. This witness statement is made on behalf of Fujitsu to assist the Post Office IT Inquiry (the "**Inquiry**") with the matters set out in the Rule 9 Request provided to Fujitsu on 11 March 2022 and a series of further questions provided to me by the Inquiry on 1 July 2022 (the "**Request**"), to the extent I have direct knowledge of such matters.
3. The topics set out in the Inquiry's Request of which I have knowledge relate to events that took place more than 17 years ago; namely the design, development and robustness of the Legacy Horizon system in the period up to the national rollout. In preparing this witness statement, I have tried to remember these events to the best

WITN04830100

of my ability. However, given the passage of time, there may be certain matters where my recollection is more limited.

4. Where I have included information from documents relevant to the Inquiry's Request, these documents are referred to using references WITN0483_01/1 – WITN0483_01/4 and are listed in the index accompanying this statement. Documents that have not already been provided to the Inquiry are exhibited to this statement.

BACKGROUND

5. I joined ICL Pathway Limited ("**ICL Pathway**") in around 1997 as a Solution Architect in the architecture and design team, focusing on infrastructure design. I continued working on the Horizon project until around 2005 when I moved to my next assignment. Prior to joining ICL Pathway, I worked at International Computers Limited as a VME (Virtual Machine Environment) Design Implementer and then for the ICL NT Centre of Excellence in Manchester from where I was seconded to ICL Pathway. I do not recall when my transfer to ICL Pathway became permanent, but it was at some point in the early 2000s.

6. During my time in the ICL Pathway infrastructure team, my work focused mainly on disaster recovery and resilience. Disaster recovery is a term used to describe the failover of service between data centres. Resilience then looks at component availability within a data centre to ensure service availability. Following my initial work on disaster recovery and resilience design, I moved into supporting the systems management design, including service monitoring and support access.

WITN04830100

7. I was not involved in the design or development of applications for Horizon. Nor was I involved in the testing or acceptance of Horizon. This statement therefore aims to answer some of the Inquiry's questions from an infrastructure perspective only.

DESIGN AND DEVELOPMENT

8. I joined ICL Pathway during the development of Release 1C, which I understand to have been rolled out to 200 – 300 Post Office branches. Branches ranged in size from single counter branches to multiple counters. At that time, the counters used a piece of software known as Riposte, which worked as a message queue; with each new transaction added to the back of the queue. Riposte was owned by a company called Escher and was selected prior to my joining ICL Pathway. My specific area of specialism in relation to Riposte was the resilience of the message store and how it was protected against failure. My view in that respect, is that the use of Riposte met the needs of the solution. I will come on to discuss how data was replicated from Riposte across the counters and to the data centres later in this statement.
9. The design and development of Horizon followed a classic waterfall methodology. Design documentation was produced, the solution was then developed, tested and deployed through releases. There were various test environments, including a resilience and performance test rig, where the team would attempt to break the system and validate the resilience design that returned service to operation. I do not recall whether Post Office provided assurances in relation to the design documentation produced.
10. In terms of factors that influenced the design and development of Horizon in the early years, when Horizon was first rolled out, the system used an ISDN (Integrated

WITN04830100

Services Digital Network) network. With 20,000 ISDN lines to install, the size and scale of the system was a challenge. The availability and reliability of the ISDN network was also not sufficient to respond to Post Office's reporting requirements – 100% of data from the counter estate needed to be received at the data centres to support reporting within four days. ICL Pathway therefore had to design a workaround to enable the necessary reporting to be undertaken. I was not involved in the design or implementation of this workaround, but I recall that it may have involved the physical attendance of engineers. As I started working for ICL Pathway after the contract was awarded, I do not know whether issues with the reliability of the ISDN network were known before the Horizon was rolled out. However, if issues were known, I would have expected to see mitigating mechanisms built into the original solution. I do not recall there being such mechanisms in place.

11. The withdrawal of the Benefits Agency from the project and therefore the benefit card functionality of the system would also have been a significant influencing factor.

12. ICL Pathway was supported by large delivery teams primarily based in the ICL Feltham and Bracknell Offices. At the start of the project, I was working in Manchester and would travel to Feltham or Bracknell each week. The initial ICL Pathway delivery team was supported by a design and architecture team, numerous development teams (supporting database application, agent application and counter development), test teams, covering both functional and non-functional requirement testing, as well as operations teams including 1st, 2nd and 3rd line support. From my recollection, there was good communication between the teams working in the ICL Pathway organisation.

WITN04830100

13. The ICL Pathway chief architect was Alan Ward who was supported by a deputy, Mark Jarosz; when Mr Ward left ICL, Peter Wiles replaced him as chief architect. The design team was initially managed by Dick Long. During my time working for ICL Pathway, the organisation went through a number of changes as it evolved to meet the needs of the solution.

14. I initially reported to Mr Ward, focusing on the resilience and recoverability of the solution. Mr Ward's team initially included four people who focused on non-functional aspects across the whole solution.

15. Following a re-organisation where application and infrastructure delivery were moved into separate teams, I moved into the infrastructure team.

ROBUSTNESS

16. I understand from the Inquiry that the term "robustness" includes:

    a. "*the accuracy and integrity of the data recorded and processed by the Horizon IT System;*

    b. *the extent to which deficiencies in the Horizon IT System were capable of causing and / or caused apparent discrepancies or shortfalls in the branch accounts;*

    c. *the ability of the Horizon IT System to identify errors in data and discrepancies or shortfalls in branch accounts and the cause of the same; and*

    d. *the ability of the Horizon IT System to continue to operate satisfactorily in the presence of adverse conditions*."

17. My involvement in the Horizon solution was limited to the design of the infrastructure supporting the application hosted in the data centres, as well as how data centre hosted applications would recover from failure. I was not involved in the design,

WITN04830100

development or testing of the application except in regard to resilience and recovery following infrastructure failures (including server failure, network failure and data loss). Neither did my role at this time involve communications with or reporting to Post Office or the Government on the subject of robustness. In light of my role, the content of this section of my statement is limited to limbs (a) and (d) of the Inquiry's definition of robustness. Due to the way in which messages were recorded in Riposte and then replicated to other counters in the branch as well as servers within the two data centres, as well as the audit records described in this statement, I did not have specific concerns relating to the "robustness" of Horizon in respect of limbs (a) and (d) of the Inquiry's definition.

18. As mentioned earlier in this statement, in Legacy Horizon, the Post Office counters used a software product called Riposte to record transaction data. To ensure a resilient record of transaction data, messages recorded in Riposte were replicated on each of the counters within a branch. The messages were then replicated through a gateway counter to the data centres, which were located in Wigan and Bootle at that time. The messages were also replicated between the data centres. Replicating the data in this way ensured that data could be recovered in the event of a disaster scenario.

19. In terms of the integrity of the data itself, because Riposte worked as a message store, once transactions (made up of individual messages) were recorded, they could not be amended or deleted. To amend the effect of a previous transaction or message, a new message would need to be added to the message store which rolled-back the effect (or part of the effect) of the original message. The original message

WITN04830100

would remain in place in its entirety; it would not be amended or deleted. I understand that this method was used by ICL Pathway support staff to make corrections on behalf of postmasters when support calls were raised. However, as I did not work as part of the support teams, I cannot comment on the mechanism by which messages were added to the message store or the processes followed by the support teams.

20. After 2000, with the introduction of Network Banking, a system was introduced to record the actions taken by support staff when accessing the solution, including the Riposte message store. This system was based upon an open source Cygwin Secure Shell product which the team modified to capture the key strokes typed by the support staff into an audit of actions logs. The audit of actions logs were retained securely in order that they could not be modified by support staff; they could only view the audit of actions logs to aid the diagnostic process. The Cygwin Secure Shell system and audit of actions logs were in addition to the message store audit described at paragraph 18 above, which had been in place since Go-Live. Much of the above explanation is set out in more detail in the System Outline Design document for the relevant Secure Support system (WITN0483_01/1).

21. The modified Secure Shell product was essentially an early example of a Security Information Event Monitoring system; it provided a record of the actions performed which was then available to the security and audit manager. This improved the record of actions taken on Horizon and supported the integrity of the data recorded. This type of functionality is commonplace in systems now but was not, as far as I was aware, expressly stipulated as part of the Requirements for the Horizon system in the early years nor was it a product that was readily available. Requirements for the

WITN04830100

Horizon solution were determined and provided to ICL Pathway by Post Office. As noted above, this Secure Support system was put in place following the introduction Network Banking. This system was not in place at the time of the national rollout.

22. The Horizon solution included an audit of all data written to the Riposte message stores. This audit data plus other information was stored in the audit service at the data centres; audit data was initially stored on tapes for up to 7 years. The tape storage solution was replaced in 2002 by a solution based upon EMC Centera technology, which allowed more rapid access to the audit data storage by the audit manager in support of Post Office audit requests. The retrieval process is explained in detail in the High Level Design document relating to audit data storage and retrieval (WITN0483_01/2), a copy of which is exhibited to this statement.

23. The introduction of the EMC Centera technology improved the time taken to access information within the audit trail. Unlike the tape based solution where data was stored on offline tapes (which I recall were stored at a secure offsite storage facility), the EMC Centera solution provided online access to the audit trail. With the tape based system, tapes containing relevant information needed to be physically retrieved from the offsite facility before being loaded onto the audit server where the data then became available to the audit team in support of retrieval requests. With the EMC Centera solution, audit data was available online and immediately accessible to the audit team (using the audit workstation), without requiring tapes to be retrieved and loaded. I refer to Change Proposal 3240 and the Audit Data Retrieval High Level Design document dated 26 November 2004 in this regard (WITN0483_01/3 and WITN0483_01/4, respectively).

WITN04830100

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated: 9/8/2022

Index to the First Witness Statement of Simon Andrew James Fawkes

	Description	Date	Control Number	URN
WITN 0483_01/1	Secure Support System Outline Design	2 August 2002	POINQ0094207F	FUJ00088036
WITN 0483_01/2	High Level Design: Audit Data Storage & Retrieval	25 February 1999	POINQ0104382F	FUJ00098211
WITN 0483_01/3	Change Proposal CP3240	3 April 2002	POINQ0123678F	FUJ00117507
WITN 0483_01/4	Audit Retrieval High Level Design	26 November 2004	POINQ0123679F	FUJ00117508