WITN00680100

Witness Name: Stephen Parker

Statement No.: WITN00680100

Dated: 27th March 2023

POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF STEPHEN PARKER

I, Stephen Parker, will say as follows…

Career History

1. I am a former employee of Fujitsu and held the position Head of Post Office Application Support. This witness statement is made to assist the Post Office Horizon IT Inquiry (the "Inquiry") with the matters set out in the Rule 9 Request dated 11th January 2023 (the "Request")

2. I started working within the IT industry at the age of 16 as a computer operator for a company providing IT services to Lloyds of London. I later moved into a system support role within this company until I joined ICL in 1985. Prior to my work on the Post Office account, I held a number of roles within ICL, including in-house operations and support roles for online systems, support consultancy services and design and development roles using Microsoft tools.

WITN00680100

3. I have no academic qualifications beyond secondary school. I have received industry specific technical and skills training. These included programming languages and methodologies, database systems, support techniques and management skills training. Having worked for the same company for many years and now being retired I have not maintained a CV for some time so do not have a list of training with that I can reproduce here.

4. I began working in July 1997 as a support consultant within the Software Support Centre (SSC) for the Pathway project (later Post Office Account (POA) and Royal Mail Group Account (RMGA)), providing third line application support for the Horizon application.

5. My technical role specialised in the support of data centre systems. Within this role I also developed some of the support tools used by the SSC and was for a few years the lead designer and part of development team for the SSC Website.

6. In addition to my technical role I also assisted the SSC manager (Mik Peach) in the provision of the support service and its operational management. Although this role never carried a formal title I effectively acted as the deputy manager to the SSC.

7. Between December 2009 and March 2010 I was a full time Problem Manager / Operational Manager of the SSC, responsible for the management of incidents through the whole support process.

WITN00680100

8. In March 2010 I became the Manager of the SSC and was responsible for the provision of third line application support to the Post Office Account, including the management of the staff working on the account. The SSC subsequently expanded to provide support services to a number of Fujitsu customers (described as “shared service”), the largest of which was still the Post Office Horizon system. As head of this unit I was responsible for strategic support for 4 customers and the management of 25-40 staff.

9. I accepted voluntary redundancy from Fujitsu and retired in December 2019.

10. In total I supported and developed IT systems for 43 years.

11. On leaving Fujitsu I did not retain any documentary information relating to the business. The information here relies on my memory and any documents supplied by the inquiry. While I do not have a good memory for dates or figures, I help here as much as I can.

Horizon Support Structure

12. The Horizon system had a multi level support structure which is common within the industry. Generally, as you move up through the levels of support the cost of the staff providing the service increases because they are more skilled and experienced. There is often overlap of skills between adjacent lines of support and while a team may be responsible for a particular level of support, staff within that team can have skills which allow them to perform a role that is more

WITN00680100

usually performed by the previous or next level of support. There were 4 lines of support for the Horizon service.

13. 1st line support was provided by a number of teams, namely the Horizon Service Desk (HSD Initially operated by Fujitsu, later moved to ATOS, I do not remember the date when this happened), the Communications monitoring team (CMT, also operated by Fujitsu) and the National Business Support Centre (NBSC, operated by Post Office).

14. Post Office outlets would contact the Horizon Service Desk for issues relating to the Horizon application or the hardware provided in branch by Fujitsu to run the Horizon application (The HSD has also been known as the HSH, Horizon System Helpdesk and the Horizon Incident Team). HSD staff dealt with enquiries such as:

    14.1. Helping sub-postmasters with the operation of the Horizon hardware, scheduling engineers to attend branches to investigate reports of hardware issues.

    14.2. Helping sub-postmasters with the operation of the Horizon application.

    14.3. Monitoring the live estate and taking corrective actions defined in knowledge documents.

WITN00680100

15. 1st line Communications Management Team operated by Fujitsu which specifically focused on communication / network incidents, both within branch and between the branch and the Horizon data centres.

16. National Business Support Centre, 1st line help desk for business / operational issues operated by the Post Office. I am unable to expand further having never seen this 1st line environment.

17. 2nd line support was provided by the SMC (System Management Centre). The SMC's responsibilities included:

    17.1. Searching knowledge articles based on the descriptions of issues reported by branches, gathering evidence and applying simple, well-defined work-arounds (often on the phone). An example of this would be resetting passwords.

    17.2. Supporting the Tivoli infrastructure which distributed the Horizon application to the counters.

    17.3. Reporting on events (alerts) generated by outlet and data centre systems. Generation of incidents based on these events.

    17.4. Operational Business Change (OBC), supporting the engineers who were opening and closing branches and increasing and decreasing the number of counters in branches.

WITN00680100

18. 3rd line application support was provided by the SSC (System / Software Support Centre). The SSC's role is defined in detail in POL00000912 (Legacy Horizon) and FUJ00080234 (Horizon online). This is a précis. SSC staff provided 3rd line application support and had a detailed knowledge of the Horizon application, they:

18.1. Applied analytical skills to the symptoms and evidence gathered by the 1st and 2nd line functions and undertook in-depth investigation into incidents.

18.2. Designed, tested and documented work rounds for the 1st and 2nd lines of support.

18.3. Investigated and resolved new Software Incidents. Undertook source code examination, complex diagnosis and documentation of new application problems before sending them to the 4th line support group for root cause software fixes. This would include the design and documentation of work rounds to mitigate impact to service.

18.4. Undertook complex configuration (configuration items can be used to alter the behaviour of the application) and data fixes which might have required the generation of special tooling.

18.5. Designed, wrote and documented new support tools. This included the development and maintenance of Peak and the SSC Web (which contained the KEL) systems.

WITN00680100

18.6. Provided technical support to other internal Pathway / POA teams working on Horizon. For example, Horizon Problem Managers, Reference Data Management, Security Operations, Release Management Forum.

19. 4th line support staff had an intimate knowledge of narrow areas of the system and were ultimately responsible for the production of permanent fixes to repair the root cause of an incident or problem in the live application. They had knowledge of computer languages and development methodologies which they used to fix problems in the live application code. There was often overlap between 4th line and development, who added new features into the application.

20. There were other teams providing support services whose roles did not fit neatly into this 4 layer model. These included:

20.1. Security Operations. Responsible for the Reconciliation Process. Business Incident Management Service (BIMS) entries. I believe the functions of another team (Management Support Unit - MSU) were subsumed into Security Operations (can't remember when) so I'm using the name Security Operations in this document to indicate either.

20.2. Belfast Operations. Operation of the Data Centre systems and the support of the operating systems running on them (e.g. Windows, Oracle)

WITN00680100

20.3. Reference Data Management. The team who tested and processed and ensured the delivery of, reference (AKA configuration) data. This team was merged into the SSC in approx 2010.

21. I have been asked about the relationship between the support teams within Fujitsu. The relationship between support groups was generally good. Secondments were arranged between units, e.g. 2nd line staff working with 3rd line, 3rd line working with testing or development to foster co-operation and understanding of each others roles.

The SSC

22. The SSC operated with various structures and numbers of staff over the 22 years I was involved:

23. During the legacy Horizon period there were between 20 and 30 members of staff in the SSC. SSC staff members would generally be referred to as diagnosticians or technicians, the two terms being interchangeable. The original SSC manager (Mik Peach) ran the SSC as a flat structure with all staff reporting directly to him.

24. Later when I took over as SSC manager (April 2010) I split the SSC into 3 teams consisting of a team lead with 6-8 members of staff reporting to them. These teams were purely administrative. The reference data team was also merged into the SSC at approximately this time.

WITN00680100

25. In approx 2014 my role was expanded to include the support of three other customers and three additional support teams came under my remit, the result being a total of six teams and some 40 staff. Changes in workload had left support teams dedicated to a particular customer under or over resourced (Horizon support was one of the areas identified at the time as being over resourced). Expanding the SSC in this way allowed more resource sharing (people and tooling) hence the SSC became known as “shared service” unit. Removing some team demarkation and cross training staff allowed an individual to support more than one customer. This improved workload resourcing and the retention of experienced staff by providing a varied and more interesting workload (particularly true for Horizon support staff). This type of sharing would also allow support tools (such as the SSC website) to be utilised in the support of more than one customer rather the‘reinventing the wheel’ for each customer. From necessity, my role became more strategic and I had less involvement in the day to day operation of the support service, this being covered by my team leads. For the purposes of this document I am only describing the facets of the SSC relevant to Horizon.

26. Over the life of the SSC staff would move on to other roles inside our outside Fujitsu. Such changes are normal and may cause short term resourcing issues while new staff and recruited and trained. At no time did I consider the SSC to be under resourced to the detriment of any of the customers we supported.

27. SSC staff received formal training on the technologies used in the applications they supported. For the Horizon application this included Microsoft Visual Basic, Riposte, Java, Oracle databases and SQL server database. Because

WITN00680100

the Horizon application was bespoke, designed and developed to Post Office requirements, Horizon application training would be delivered to the SSC by the development teams as and when new facilities were introduced. This process was often referred to as “knowledge transfer". SSC diagnosticians would also be expected to self train by examining design documentation and support guides produced as part of the Horizon development process.

28. Turnover of staff within the SSC was quite low. When replacement or additional staff were needed preference would be given to people within other Fujitsu departments with a relevant technical background. If such people were not available a standard CV / interview process would be followed to recruit externally. Any successful applicants working on Horizon were subject to security vetting and approval of the Security Operations team. There were no academic criteria applied to the recruitment process, selection criteria were technical ability, being based on a combination of:

28.1. Previous experience within a support environment

28.2. Knowledge of the core technologies used for the application being supported.

29. I have been asked about the role of SSC Manager: This was a wide role encompassing the day to day operational management of the SSC, staff welfare, development and strategic direction for the Horizon support function. The SSC manager’s responsibilities included:

WITN00680100

29.1. Staff welfare

29.2. Staff career development. Regular appraisal of staff.

29.3. Day to day resourcing.

29.4. Problem management.

29.5. Workload prioritisation.

29.6. Support service reporting.

29.7. Support service analysis and improvement.

29.8. Interface to other departments.

29.9. Representing support in the software release process.

29.10. Authorisation for the production of new support tooling.

29.11. Authorisation of operational changes (OCRs and OCPs).

29.12. Generation / amendment of work instructions.

30. As I have mentioned before, the SSC did not have a formal role called “deputy manager” while Mik Peach managed the unit but there was a requirement for a stand in for the SSC manager to make the day to day decisions required to

WITN00680100

keep the SSC running in the managers absence. This was the role (in addition to my support role) I fulfilled during the time when Mik Peach was the SSC manager.

31. The vast majority of the Horizon work into the SSC was recorded as Peak incidents. Other "ad-hoc" tasks could originate from problem managers or other departments within Pathway. Sometimes a person (e.g. Problem Manager) would request work directly from their favourite SSC diagnostician but this was discouraged.

32. The SSC administrator (Barbara Longley and later Lorraine Elliott) would assess each Peak as it arrived and allocate it to members of the SSC based on their skills and current workload. This may also include a revision to the priority. The SSC administrator role was not technical. The SSC manager allocated any requests for other work not recorded on Peak.

33. In approximately 2010 (I cannot remember the exact date) this method of allocation changed. The workload of the SSC administrator had decreased over time and the account economised by removing the role. A daily rota of SSC diagnosticians was established, known as the "Prescan Rota". The diagnostician on Prescan would assess each new Peak incident, immediately responding to those which required little work or allocating the incident to another member of the SSC, again based on their skills and current workload. The "Duty Manager Rota" was also established, staffed by SSC team leaders. This role processed operational issues: accepting and allocating ad-hoc

WITN00680100

requests, sign off operational changes. Neither of these changes had any adverse effect on the Horizon support service.

34. Incident priority was initially allocated by the originating team or service. After a technical evaluation was completed the priority may be amended by the SSC if the initial value was inappropriate. There was guidance on the priority for an incident in the "End to End Support Strategy" document (FUJ00080212) but is was essentially determined by and evaluation of:

34.1. Impact to user / service

34.2. Number of users / systems affected

SSC Website

35. The SSC developed and supported an internal (to Fujitsu) website to store and allow the rapid retrieval of, support knowledge, operational change details and general information for the Horizon support community. This has been variously known as the SSC Intranet or SSC Web. The SSC Web was developed and improved over the life of Horizon and was the main support knowledge base for the Horizon system.

36. One type of knowledge entry held within the SSC Web was the KEL (Known Error Log): KELs record support knowledge which is intended to assist staff in the support and understanding of the Horizon system. KELs could be created and updated by Horizon support, test and development. There was one

WITN00680100

exception, the 1st line help desk function do not create KELs (HSH 1st line used their own knowledge base).

37. While each KEL was constantly updated to provide the best current technical information, they did not contain the history of an incident. This was documented on the Peak (AKA PINICL system) system.

38. KELs were generated for a number of reasons while I worked on Horizon, for example: to explain system behaviour or messages that originate from central and counter systems; to record actions that technicians may take to determine the reason for a system behaviour or gather relevant evidence to aid understanding; to provide guidance on which document to read to understand a particular aspect of the system; to record symptoms and outcomes from incidents referred by other support units; to record support information on issues seen in test environments.

39. The acronym KEL is a misnomer inherited from a previous system. KEL entries were support knowledge entries and did not have a one to one relationship with errors on the system. There were a more KELs which contained technical information designed to assist in the understanding of the system than KELs relating to specific application errors.

40. When attempting to resolve an operational issue or a reported incident the diagnostician would use the text searching facilities of the SSC Web. The diagnostician would use their experience to identify keywords to describe

WITN00680100

whatever is being investigated and then use these words to define search criteria.

41. After being presented with search criteria, the SSC Web would examine the knowledge base and return to the diagnostician summary entries from documents, work instructions and KELs containing information matching the search terms. The diagnostician would then examine these summary entries in detail to ascertain relevance to the problem being worked on.

42. The textual search function was invaluable in reducing the large volume of information held within the SSC Web to a small subset that was of use to the diagnostician seeking information on a particular subject.

Operational Change

43. The SSC Website also contained the operational change platform. Operational change documents were used to record the detail of operational changes and provided a vehicle for the assessment of their potential risk / impact and approval to proceed.

44. Documents were called OCPs and OCRs. One allowed the SSC to record minor changes that only required SSC manager approval, the other was for changes with wider impact that required the notification and approval of multiple teams. Examples of the types of changes OCP / OCRs were used for include: configuration changes, system reboots and hardware replacements. I cannot recall all the types of change that were recorded on OCP / OCRs or the

WITN00680100

detailed content and scope of any data corrections. More clarity for the inquiry could be obtained from Fujitsu.

45. Each team would assess the change described and document on the OCP / OCR:

45.1. Potential risk / impact to the teams area of responsibility.

45.2. Scheduling of resources required of their team to implement to change.

45.3. Formal approval from team to proceed with change.

46. The SSC manager (or delegate) would approve OCPs / OCRs on behalf of the SSC.

Peak

47. Peak was a web based software incident and problem management system used by Post Office Account for all development, test and support teams except the 1st line help desk. It enabled details of the incident and diagnostic progress to be captured in a searchable format and allowed the tracking of problems from detection through to resolution. Peak was developed in-house by the SSC from the PinICL system it replaced in 2003. The system was customised and enhanced by the SSC during the whole period of my involvement with Horizon support. John Simpkins was the main designer and developer of this system while I was SSC manager. I understand from him that

WITN00680100

this system is still in use. Peak was bespoke, it was adapted as and when requirements changed for Horizon incident and problem management. This made a Peak an excellent tool to manage Horizon incidents.

Support Process

48. The chain of support teams and the support process for resolution of an incident is described in FUJ00080212 (End to End Support Strategy), a document written by myself in 2011 which was itself derived from FUJ00079897 (End to End Support Process Operational Level Agreement) written by Mik Peach in 1999 (amended 2003) for Legacy Horizon. I have been specifically asked to include the support process in my witness statement so have produced a short form here.

49. For most of its life cycle an incident was assigned to a particular support team and a person within that team who was responsible for the next action on the incident. As the incident was progressed by various members of the support community, they added textual comments and supporting evidence to the incident record (Peak). These comments charted the progress made in resolving an issue and would vary in fullness and clarity.

50. I will describe what happened when an incident arrived when Legacy Horizon was live. Prior to the establishment of a Prescan function, the SSC administrator checked the basic details logged to the incident and assigned the incident to a diagnostician with appropriate skills. That diagnostician would do

WITN00680100

a technical analysis which might result in passing the incident (with agreement) to another member of the team with more appropriate skills.

51. I will now consider what happened once the prescan function had been implemented. The prescan diagnostician used their technical knowledge for a basic assessment of the incident. This may have resulted in an immediate response in situations where the incident was known (e.g. subject to a KEL or support guide information) or where there was inadequate information logged (e.g. basic details missing such as a FAD code) for the SSC to progress the incident. If no immediate response was possible, the incident was assigned to a diagnostician with appropriate skills for further analysis.

52. The diagnostician used their technical knowledge and expertise with the Horizon application to examine and resolve incidents. They would also examine various sources of additional information such as:

52.1. Viewing logs (log files record any significant action or occurrence that's recognised by the software system).

52.2. Accessing Horizon systems

52.3. Searching the SSC website

52.4. Searching Peak (for similar incidents)

52.5. Talking to the person who reported the fault

WITN00680100

52.6. Discussing the incident with colleagues, e.g. other diagnosticians, developers, design authorities

53. Relevant information and evidence from these sources would be added to the Peak incident as it was gathered.

54. If the diagnostician believed that the incident represented a fault in the application they may examine design documentation (sometimes a perceived fault is actually a requirement of the system design) and source code (SSC had access to all application source code) to determine the root cause.

55. In the vast majority of cases this process would result in the resolution of the incident by the SSC. The SSC diagnostician would inform the originator of the incident and / or organisation contact, such as Post Office via Fujitsu Service Management, and then apply a final response code along with summary text that supported the response code to close the incident.

56. Final response codes were used to classify the outcome of an incident and were the subjective opinion of the person closing the incident. They were useful to assess the performance of support units.

57. The 2nd line support groups were expected to answer any incidents within their operating remit (for example all user or known errors). They were also expected to send only one example of a suspected new software fault to 3rd line, retaining any duplicates at 2nd line for closure once the main incident was resolved. Because of this, any answers from 3rd line with response codes

WITN00680100

such as User Error, Published Known Error or Duplicate call would be classed as "black marks" and counted against 2nd line support (similar measures existed between 3rd and 4th line). In the SSC these measures would be reviewed on a monthly basic to assess the effectiveness of the service. I believe similar reviews look place in other departments.

58. The 1st and 2nd line groups were effective responding to incidents, this being reflected in the volume of incidents sent on to the SSC which represented a single digit percentage of the incidents originally received by 1st / 2nd line. This does not imply that all incidents sent to the SSC were suspected application errors. Incidents would also be sent to the SSC where the originating unit did not have the skills, tools or system access required to progress the problem.

59. The use of response codes as a measure would sometimes cause discussion between levels of support staff ("why did you close this as a known issue when we couldn't see the document", "why no fault in product when we don't have access to xxxxxxxx data which was essential"). These minor complaints would be resolved individually.

60. The use of response codes as a measure of support effectiveness could also lead to inappropriate response codes being used in order to “be kind” to, or prevent contention with, other lines of support. For example, “Advice after investigation” being used in preference to “No fault in product” or “Advice and guidance given”.

WITN00680100

61. If the SSC diagnosticians' investigation determined that the incident represented a fault outside the purview of the SSC the incident would be sent on to the appropriate team. For example, server operating systems issues (to Belfast Operations team) or event management problems (to Management Systems Support team)

62. If the SSC diagnostician determined that an application fix was required the incident would be onward routed to 4th line. A KEL would be raised / updated by the SSC with details of the issue. This ensured the visibility of the issue to other support groups.

63. A new problem would be discussed with the relevant business owner and the relative importance, impact and priority would be assessed (part of the Release Management function).

64. 4th line were responsible for designing and coding any fixes required to the Horizon system. They were part of the development group and had their own detailed process and procedures which I am not able to expand on.

65. Once a suitable fix had been written it would be delivered to a test system for functional and regression testing. There may be an iterative process between 4th line and test as the fix was refined.

66. Once the test team had signed off the fix as being fit for purpose, it again become subject to the Release Management process, which delivered the change into the Horizon estate.

WITN00680100

67. There was never any pressure applied to the SSC to hide application errors. The opposite was true. The SSC would push for the resolution of errors in order to improve Horizon and reduce incident workload being passed through the system. The SSC provided details of identified bugs errors and defects via the Service Management Team within Fujitsu and not directly to sub postmasters or the Post Office.

68. I now consider the mitigation of operational problems and application errors.

69. When the root causes of problems were identified, the SSC would check the Horizon system for the fingerprint left by the problem and identify which outlets were impacted. If the impact was financial the SSC would also quantify that financial impact. I have been asked to explain this in more detail which is best achieved by a fictitious example: Investigation of an incident identifies that an application error results in the recording of two stamp sales when the sale of a first class stamp happens immediately before a withdrawal of exactly £55 in cash when another 1st class stamp sale was cancelled in the same basket of transactions. Once the cause and effect are understood in this detail, the SSC could construct one of more queries, across transactions from all the counters in the Post office estate, to identify which offices exhibited exactly the same set of circumstances.

70. This information would then be collated for reporting to the Post Office by Fujitsu's Service Delivery team or Security Operations. While not my area, I have a basic understanding of how it worked:

WITN00680100

70.1. For minor issues, the information would usually be provided to Post Office by email

70.2. For major issues, it would be provided in a Major Incident Report or something similar.

70.3. Information may also be passed to Post Office via the Business Incident Management Service (BIMS)

71. As I understand it, there were a number of ways in which Post Office could take corrective action based on this information and how it choose to do this depended on the nature of the issue. One way was by issuing a Transaction Correction to restore the branch to the correct position.

72. The SSC was hugely reluctant to change transaction data as that was not our job and we recognised the seriousness of doing so. In the rare circumstances when it was necessary to correct financial information on the system we would:

72.1. Ensure that the reason for change and content of the change was approved, normally via an Operational Correction Request (OCR)

72.2. Ensure that changes were attributable to the support group by annotation within the changed information to ensure it was visible in the audit trail.

WITN00680100

72.3. Ensure that the content and execution of the change was witnessed by a second person.

72.4. Ensure POL and / or the sub-postmasters were informed (again via the Service Delivery Team).

SLAs

73. The SSC had no direct service level agreements (SLAs) or penalties (but see 74 below) relating to support incidents. The SSC did work to targets based on the priority assigned to a particular incident and the final response codes. Measures against these targets being used to determine the effectiveness of the SSC (and other support units).

74. Other services did have SLAs and penalties. The same level of diligence was applied by the SSC to all incidents, whether an SLA was relevant or not. The possibility of financial penalties was never a factor for the SSC. Particular memorable SLAs to me are:

74.1. SLAs for business incidents (owned by Security Operations) were relevant when the SSC was providing technical support to Security Operations. Business incidents (BIMS) were always treated with the highest priority within the SSC.

WITN00680100

74.2. SLAs for delivery of transactional data (I think resulted in penalties against the data centre operations service). Again, the SSC provided support here and incidents were treated with appropriate priority.

Support Tools

75. Various tools were available to the SSC to aid support of the Horizon system. Some that I remember are:

75.1. Smiley support tool written by John Simpkins (SSC), which amalgamated information from various sources (e.g. databases) into a single view pertinent to a particular support task and provided a unified interface to run various tools to achieve a single support outcome.

75.2. A Legacy Horizon tool (I cannot remember its name) written by Richard Coleman (ex SSC) whose function was to retrieve messages (i.e. data) from the Correspondence Server to local text files for examination and which was eventually subsumed into the Smiley support tool.

75.3. HORIce (Horizon Information Centre): A web based tool that eventually replaced Smiley for Horizon Online. Like Smiley, used to present read only views of database information (BRDB, APS, TPS etc) and the amalgamation of various data sets to present information to the diagnostician. Because it was Web based it allowed information to be made directly available to all Fujitsu support groups and even Post Office help desks. HORIce users expanded over time so I cannot

WITN00680100

define exactly who had access and when. Fujitsu may be able to provide a timeline by examining the users and when they were introduced.

75.4. TIP Repair Tool: Used for support work on the interface files sent from Horizon to Post Office (Chesterfield).

75.5. Audit Information: The SSC could make audit retrieval requests via the security team (known as ARQ requests, I can't remember the meaning of the acronym) to examine system information outside the window that was directly available online from Horizon systems (3-6 months).

Remote Access

76. A computer system with geographically separated components needs to support remove access to those component systems. This remote access allows suitably trained staff to maintain the system and assist the users of that system from a distance. This support requirement has to be balanced with the necessity of keeping the system secured, ensuring that only authorised persons have access and maintaining a record of any actions taken.

77. As the Horizon system was developed and used the understanding of support and security requirements evolved. It was common for the security and support staff to discuss both requirements (support vs security) and agree on how the access rights, audit trails and security of the system should change.

WITN00680100

78. There were five teams I remember having remote access to the Horizon system which I have described below. I do not know what system components (files, databases, network shares) or access level (read, write etc) each team had once remote access has been achieved:

78.1. SMC: Access to counters and servers via a restricted Tivoli toolset (mini applications designed to return specific information or effect a carefully defined and restricted change). Used to support software distribution issues.

78.2. Belfast Operations staff (responsible for infrastructure and operating systems support). Remote and local (i.e. physically in the data centre) access to servers. Used for the support of hardware, operating systems and data centre server applications. I don't believe they had remote access to counters.

78.3. SSC: Access to counters for Riposte and reference data support. Access to data centre server applications (e.g. Oracle database), with the exception of Audit systems, for application support.

78.4. Security Operations: Access to audit information via a restricted toolset. Access for security assurance and audit data extraction.

78.5. Reference data team: Access to reference data definition (RDMC) and delivery (RDDS) systems.

WITN00680100

79. SSC remote access to counter systems has never included the ability to use the counter application seen by sub-postmasters (i.e. interact with counter screen / keyboard).

80. All technical members of the SSC had the ability to remotely access Horizon systems (This excluded the SSC administrator and Manager) under strict security controls. Security controls for Legacy Horizon remote access included:

80.1. Staff vetting. Carried out and reported on by the Security Team.

80.2. Terminals capable of remote access being held on a secure floor to which only SSC staff had access (Other staff were signed in and escorted).

80.3. Access roles required to enable remote access also required the use of a physical security token in addition to username / password.

80.4. Computer terminals with a secured operating system build (separate to standard corporate workstations).

80.5. A secured and monitored network between SSC terminals and the data centre.

80.6. The changes of system design implemented as Horizon Online made it possible to relax some of these security controls (80.2, 80.4 above). I

WITN00680100

do not have the detailed security background to explain why these changes were possible but they would have only been allowed with the agreement of the Security Architect and Security Team.

81. I have been asked to consider a document titled Secure Support System Outline Design (FUJ00088036). In the early stages of Horizon the methods used to remotely access data centre and counter systems could be described as “needs must” in order to provide the support necessary that kept Horizon running. This involved the use of a Microsoft tool “rclient”. While this tool allowed remote access and command execution on Microsoft operating systems (as used on Horizon counters and some data centre systems) it did not provide the detailed level of accountability (e.g. detailed command logging) required for Horizon. FUJ00088036 describes how the security of the system was enhanced using Secure Shell (AKA SSH, OpenSSH).

82. As a result of implementing the changes described in FUJ00088036, support access was improved while also providing enhanced levels of access security and logging. I would expect that the rclient application was removed from the system after these changes were implemented but cannot confirm that was the case.

83. I cannot give the inquiry much technical detail on the usage once remote access had been established to a counter. I was never a counter specialist but in brief I do remember remote access being used to resolve:

WITN00680100

83.1. Legacy Horizon only: Incidents affecting the replication of Riposte messages between counters in the outlet, between single counter outlet disks (master and slave) and outlet and data centre.

83.2. Incidents relating to service control parameters (reference data).

83.3. Incidents relating with the distribution of new software to the counters.

84. Remote access has always been essential to the maintenance and support of Horizon counters and servers. In particular Legacy Horizon exhibited issues that would require SSC diagnosticians re-play Riposte records into a suitable Message Store or insert new control records. Note: I am using the terms records (an entry within the Riposte Message Store) and transactions (information contained within a record that pertains to an interaction at a counter). To be clear, these SSC workarounds did not involve the construction or amendment of transactions. SSC would be re-playing records that had already been committed to a Message Store but that for some reason, were not in the correct place (i.e missing from one Message Store but present in a replicated copy). It is also worth mentioning here that the Riposte system did not allow any editing or deletion of records in the Message Store once written.

84.1. Some issues required that the SSC insert Message Store records that controlled the system state (e.g. Login / logout) or the system configuration (reference data). In most cases these records would be inserted into a Message Store at the data centre so that they would be replicated down to the outlet counters next time the outlet connected to

WITN00680100

the data centre, effecting whatever state change was required at the outlet.

84.2. Remote counter access would be used when Message Store intervention required that the records being re-inserted originated from the outlet counter. For context, records within the Riposte message store included details of the originating FAD code and counter ID. Some types of records (normally transactions) could only be accepted by the system if they originated from an ID within the outlet.

85. One would have to concede that where the SSC used Riposte tools and remote access to have a positive effect on outlet information, the opposite must also be possible. If an SSC diagnostician made errors when re-playing message store transactions then a discrepancy could result. Controls offered some protection here:

85.1. The system enforced rules which prevented duplicate or erroneous records being written.

85.2. Any such intervention would be with the sub-postmasters consent and the sub-postmaster would use system reporting to check that the results of SSC work were as expected.

85.3. SSC staff were competent in these areas (or when someone new was training they would be closely supervised).

WITN00680100

86. Unauthorised / malicious use of these tools by a member of the SSC was possible but I cannot see the motivation for this. There would be no financial incentive without collusion with the sub-postmaster, who could enter the same type of transactions anyway without requiring SSC assistance. I do not remember any examples of unauthorised or malicious use of remote access while I was working with Horizon.

87. Horizon Online, by virtue of its design (no transaction data stored remotely), reduced the use of remote access to counters. There were tools which allowed authorised users audited access to insert corrections to the Branch Database but I never used them and do not remember the details of them.

88. I believe audit information was held in respect of remote access but I cannot remember exactly what was collected or how it was collected.

89. I do not know who in the Post Office was aware of the remote access used by the support teams.

90. I have been asked to consider an email chain on 25th June 2015 (FUJ00087151) and in particular the comment contained within that “Access from terminal server to counter is not audited”. Unfortunately I do not remember this meeting but after reading the email I can say: The email documents the security of Horizon counters (Horizon Legacy and Horizon Online) within branch. I think it was intended to illustrate just how impractical unauthorised remote access would be. The “Access from…..” comment describes the fact that there was no audit trail in Horizon Online which

WITN00680100

documented when a network connection was made from a terminal server in the Horizon data centre (AKA SSN server) to a branch counter.

Bugs, errors and defects

91. I have been asked to comment on a number of bugs, errors or defects identified in Appendix 2 of Bates and others v. Post Office Limited (No. 6) "Horizon Issues". Unfortunately, with the passage of time, I have no recollection of the incidents quoted. Even with access to contemporary notes and documents I do not feel I would now be able to produce something useful to the inquiry. The detailed technical knowledge required is a perishable skill. The most effective way for the inquiry to get further clarity on these issues would be via Fujitsu technicians still involved with the system analysing the contemporary documents and reporting on each incident.

Reconciliation Service

92. Day to day execution of the service and reporting were the responsibility of the MSU / Security Operations team. If I remember correctly the MSU were merged into the Security Operations team (not sure when) so one may find either name being used in documents.

93. SSC involvement with the reconciliation service was limited to the provision of technical support. Examples being:

WITN00680100

93.1. Resolution of incidents preventing the provision of the service such as failures in the production of regular reporting.

93.2. Examining the live service to provide information to Security Operations.

94. As a problem manager I was very aware that any incidents relating to the reconciliation service were to be treated as a high priority (due to SLAs impacting Security Operations) and ensure they were scheduled accordingly. As a technician I do not remember the details of any incidents of this sort.

95. Service reporting and analysis were the responsibility of the Security Operations team so I am unable to comment on the effectiveness of this service.

96. The BIMS system was administered by the Security Operations team (SSC had no access) so I can offer no further detail on its operation.

Release Management Service

97. The Release Management team was responsible for the Release Management Service, which managed the scheduling of fixes and the delivery of new application modules to all Horizon systems. Regular meetings (the Release Management Forum, RMF), attended by the SSC, allowed for the discussion and dissemination of, release information:

WITN00680100

97.1. Discussion of the relative importance, impact and priority of new fixes or new functionality.

97.2. Reporting the progress of fixes and new releases (containing additional features and bug fixes) through development and test teams.

97.3. Reported on the extent to which a new release had been delivered to the server and counter estate. New software could take many days to be delivered and implemented across all counters.

Audit

98. Post Office obtained data for prosecutions from audit via the Security Team (ARQ requests). The gathering and storage of audit data was not supported by the SSC (it was supported by development). This was a deliberate security policy so that people supporting the system did not have direct access to audit information. SSC would be consulted for technical explanations of some data. In particular SSC would check system event messages retrieved as part of the ARQ and comment on any that could indicate an impact to financial data. I do not remember the content or format of the data returned from ARQ requests. Because the SSC did not support audit I am also unable to give the inquiry any help with the methods used to gather audit information or details of the information retained.

Robustness of Horizon

WITN00680100

99. I have no experience of any other application system of comparable size and complexity on which to base a comparative judgement on the robustness of Horizon. I can say:

100. During the early years of Legacy Horizon there was a great deal of support work. Staff worked long hours and in particular Wednesday evenings were always busy as SSC staff were helping sub-postmasters with their cash accounts / rollovers. I don't consider this to be an indication of a lack of robustness, in the early days support staff were getting used to a new system and as the national rollout progressed, new sub-postmasters were being introduced each week who also had to get used to the system.

101. I also noticed a change in supportability between Legacy Horizon and Horizon Online:

101.1. Legacy Horizon logged all transactions locally and only communicated with the data centre intermittently. This localised design was necessary when computer networking was in its infancy but could present issues to the integrity of transaction data if not correctly managed. Risk was mitigated by replicating data between counters or multiple disk drives to provide multiple copies of information. This design did increase the amount of intervention by required by support groups to ensure transactions were visible to the system in the correct place and at the correct time. This work did not involve the construction of transactions.

WITN00680100

101.2. The improved availability, speed and reliability of network connections allowed Horizon to go totally online (Horizon Online), all transactions were processed in the data centre. This design change improved the supportability of the system and reduced the amount of intervention required from support staff.

Advice and assistance

102. I have been asked specifically to comment on the sub-postmasters access to adequate advice and assistance. The majority of advice and guidance was provided by the Post Office (e.g. NBSC, branch visits) and 1st line support (HSH). Since I had no direct involvement I cannot help the inquiry with these areas. In the cases when the SSC contacted sub-postmasters directly, I believe that all required assistance was given.

SSC involvement with prosecutions

103. SSC had very little involvement with prosecutions. This changed briefly when Anne Chambers was persuaded to write a witness statement because she had provided some assistance with a particular incident. She subsequently also made a court appearance as a witness. I remember that she found this stressful and her experience made people in 3rd line think twice about providing support for certain kinds of issues. As a result of this, Gareth Jenkins (Horizon architect) was nominated as, for want of a better term,“court representative” and the SSC's role was limited to fulfilling his requests for

WITN00680100

information from the live system (Gareth, as part of the architectural team had no live service access).

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated 27/3/23

Index to First Witness Statement of Stephen Parker

No.	URN	Document Description	Control Number
1	POL00000912	CS Support Services Operations Manual	VIS00001926
2	FUJ00080234	Horizon Online 3rd Line Application Support Service: Service Description	POINQ0086405F
3	FUJ00080212	Fujitsu "End to End Application Support Strategy", version 1.0	POINQ0086383F

WITN00680100

4	FUJ00079897	Fujitsu Services End to End Support Process, Operational Level Agreement, Version 2.0	POINQ0086068F
5	FUJ00088036	Fujitsu Services: Secure Support System Outline Design v1.0	POINQ0094207F
6	FUJ00087151	Email from Pete Newsome to Harvey Michael and Gavin Bell re: FW: 3 scenario demo	POINQ0093322F