Witness Name: Michael Edward Pryor Peach

Statement No.: WITN04510100

Dated: 3 March 2023

POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF *MICHAEL EDWARD PRYOR PEACH*

I, *MR MICHAEL EDWARD PRYOR PEACH*, will say as follows:

INTRODUCTION

1. I am a former employee of Fujitsu Services Limited (**Fujitsu**). I left Fujitsu in September 2009.

2. 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 provided to me on 6 January 2023 (the **Request**), to the extent I have or had direct knowledge of such matters. I was assisted in preparing this statement by Morrison Foerster, who represent Fujitsu in the Inquiry.

3. The topics set out in the Request concern events that occurred over 13 years ago. I have set out my best recollection of these events in this statement, which relate to (a) problem and incident management systems, (b) the Software Support Centre (**SSC**) at Fujitsu, (c) Escher and Riposte, (d) bugs, errors and defects (**bugs**, each a **bug**) in the Horizon IT system (**Horizon**), (e) remote access, and (f) the conduct of prosecutions by and on behalf of Post Office

Limited (**POL**). While I have tried my best to recall these events, due to the time that has passed, there are areas where my recollection is unclear or limited.

4. As requested by the Inquiry, I have reviewed the documents referenced by the Inquiry in the Request. I have also refreshed my memory by reviewing other contemporaneous documents made available to me by Fujitsu. Where my recollection has been either supported by or prompted by documents, they are referenced using the Inquiry's Unique Reference Numbers and are set out in the index accompanying this statement.

BACKGROUND

5. I was first employed by ICL PLC (**ICL**) in 1980. Initially, I was in regional technical support for customers using the Virtual Machine Environment (**VME**) operating system. Later, I transferred to the VME Network System Support Centre unit in Bristol as a Network Support Diagnostician. I then became manager of the VME Base System Support Centre unit, based initially in Reading and then Bracknell. Both of these units—the VME Network System Support Centre and VME Base System Support Centre—were part of the ICL Customer Service team (**ICL Customer Service**).

6. Following my role as manager of the VME Base System Support Centre unit, I spent a brief period as a project manager in ICL Customer Service, introducing the PC-PARIS product, which was a Known Error system supplied to ICL support units and to VME customers. This Known Error system was unrelated to Horizon. Still working within ICL Customer Service, I then headed a small Rapid Application Development (**RAD**) team based in Bracknell which specialised in delivering short-term development projects to ICL Customer

Service. This RAD team was not part of ICL Pathway Limited (**Pathway**), and did not develop any code or applications for Horizon.

7. I left the RAD team and ICL in 1997 to join Pathway in Feltham as the Manager of the SSC (3rd line support). I held this role until I left Fujitsu on 30 September 2009.

8. My work and involvement with Horizon was almost exclusively concerned with the Horizon system that first went live in 1999–2000 (now known as **Legacy Horizon**). Legacy Horizon was replaced by a new system (Horizon Online or **HNGX**), which was in the process of going live when I left Fujitsu.

KEL SYSTEM

9. The Known Error Log (**KEL**) system was designed and written within the SSC. The purpose of the KEL system was to provide information about errors reported on Horizon. As I recall, the system was accessible by all Pathway (and later Fujitsu) Post Office Account (**Post Office Account**) units including support, testing, development and management support. These units could raise a record of a “known error” on the KEL system, and we referred to these individual records as “a KEL”.

10. The system was written primarily by Steve Parker, who had a great deal of support experience, and experience of previous Known Error systems, which he used to develop a system that was accurate, used full text searching capabilities, and was easy to use. The KEL system documented the symptoms of the incident, and Systems Management Centre (**SMC**) (2nd line support) would enter the symptoms into the system as closely as possible to what the customer (usually a postmaster) had described. By logging symptoms as

described by customers rather than technical staff, the system was designed to find more “hits” if other customers reported similar symptoms recurring.

11. Units outside the SSC were encouraged to use the system. In particular, the SMC were encouraged to raise a KEL for any calls (i.e., reports of an incident) which were to be passed to the SSC. The SSC staff would then update the KEL. If the issue which prompted the KEL was resolved, the resolution would be appended to the KEL. If the issue was unresolved because the evidence required to assist diagnosis of the fault was insufficient, then the evidence that was required would be documented on the KEL. In order to search for a similar error on the KEL system, all that needed to be done was to type into a text search box—essentially the same as a “google” search.

12. I believe the KEL system was adequate for its purpose because it did what it was designed to do, which was to provide a way for support teams to confirm whether an incident that was being reported by a customer was a known issue. It was also designed and developed by the people who most used it.

PINICL AND PEAK SYSTEMS

13. When I joined Pathway, the PinICL system was in use, but it was ageing. It was used to record the details of incidents and to allocate them to development, and later support teams. I was not involved in the design or development of PinICL, and only used it for a short period of time, which I cannot recall, and I cannot comment further.

14. Since PinICL needed to be replaced, the decision was taken to develop the Peak system. This work was done by the SSC for a number of reasons: (a) the SSC were likely to be the people who most used the system, (b) some SSC

staff had experience of development, (c) I had experience managing staff developing Helpdesk systems, and (d) the SSC staff had experience of PinICL and could therefore retain much of the "look and feel" of PinICL.

15. The process by which a call (which we also referred to as a "Peak") arrived in the SSC was as follows:

    a. An incident would be logged by the Horizon System Helpdesk (**HSH**, later called the Horizon Service Desk or HSD) on Powerhelp (an externally purchased Helpdesk application). Incidents coming into the HSH could have originated from postmasters, other units within the Post Office Account, or POL. Other Fujitsu units that were dealing with Horizon, including MSU, development and testing would raise calls direct onto the Peak system. The Network Business Support Centre (**NBSC**) would send calls by contacting the HSH.

    b. If the incident was suspected to be a software issue, it would be passed to the SMC, who would perform KEL checks (i.e., check the KEL system) and other diagnosis.

    c. If, after their diagnosis, the SMC considered the incident to be a software issue, the incident would be passed to the Peak system via an Open Teleservice Interface (**OTI**) and arrive in the SSC.

    d. The SSC Coordinator would allocate the call to a member of the SSC's technical staff (their formal title was "Product Specialist", but we would often call them SSC technicians) based on their area of expertise (Counter, Agent, Database, etc). Initially, the SSC Coordinator allocated calls based on their knowledge of the areas of expertise of the SSC technicians, and if they were unable to determine which area of expertise was most appropriate for a particular call, they would speak to myself or the SSC technicians for guidance. Later on, I produced a skills matrix for all members of the SSC to assist the SSC Coordinator with the allocation process. The SSC Coordinator would also consider the workloads of the SSC technician when allocating calls—usually the number of incidents the technician was managing at the time, and sometimes I would tell the SSC Coordinator not to pass calls to specific technicians for reasons of workload.

e. The SSC technician would then analyse the incident and attempt to resolve it. If the incident was resolved, it would be closed on the Peak system, which in turn passed the closure details back over to Powerhelp via the OTI. If the incident was identified as a code error by the SSC, the SSC would forward the call to the development team responsible for that part of the system, usually after discussion with the specific developer as to exactly what evidence would be required in order to identify the exact area of code in error.

f. Incidents were also raised by other staff in Pathway's (later Fujitsu's) Customer Service team (**Customer Service**), and by testing and development teams. These were raised direct onto the Peak system. For example, receipts and payments mismatches would be raised by the MSU. In the case of the testing teams, the incident would be raised and then passed to the development unit responsible for the part of the system in question.

g. Prioritisation of incidents which arose from the 1st and 2nd line support units (HSH and SMC, respectively) was done prior to the incident arriving in the Peak system. So, except for incidents raised by the SSC, neither myself nor SSC staff were responsible for allocating the priority of an incident. The SSC could later change the priority if, for example, an incident reduced in urgency as a workaround had been put in place. The SSC would also upgrade a call if it became more urgent, but I do not recall it happening often.

h. Evidence for an incident was generally obtained by SSC technicians accessing the live system through secure PCs (**SSC PCs**) attached to a secure Local Access Network (**LAN**) connecting to the data centres. The SSC had dedicated servers in the data centres for the storage of evidence, but I do not recall the exact mechanism by which the data was "attached" to an individual Peak. I do recall that on a number of occasions, development staff would visit the SSC secure area in order to look at evidence from the live system. When gathering evidence, access to the live system would be on a "read only" basis. Development staff did not have access to the live systems and would need to visit the SSC secure area to view diagnostic data.

i. Where an incident was reported from development or testing teams, these teams were able to attach the evidence to the Peak itself.

j. An incident would be considered closed once the root cause had been identified and a remedy put in place. The remedy would differ depending on the nature of the root cause. For example, an incident requiring a code fix would remain open until such time as the fix had been tested and applied to the live estate. Other closure categories may have required different closure actions.

k. When an incident was resolved on Peak, it would be returned to the SSC, who would then close it. This in turn caused the incident to be reported as closed over the OTI link to Powerhelp.

16. I believe the Peak system was more than adequate to manage incidents on Horizon because enhancements were made to the system that went beyond its original scope of managing incidents. Furthermore, since the Peak system was internally developed, it was also capable of rapid change should additional requirements be requested by other units in Fujitsu involved with Horizon.

Service Level Targets

17. I am aware that there were Service Level Targets (**SLTs**) in the contract between POL and Fujitsu, and I recall that the majority of these SLTs related to hardware, including timescales for replacement, engineer response times, and network availability. These would still be "service tickets" but would be handled by HSH and SMC and would only relate to PinICL or Peak if a hardware or network call were passed to the SSC in error.

18. There were SLTs relating to the processing of transaction data which indirectly impacted Peak. Fujitsu were targeted with processing high percentages of transaction data from Post Offices into the Fujitsu data centre systems within a

certain number of days. My recollection is that when it was recognised that a Post Office branch had not reported their "end of day", a Peak would be raised and passed to SSC to investigate the reason. I recall that SSC staff developed a script to run on one of the data centre servers to report all missing "end of day" markers.

19. I recall that all of the SLTs in the contract contained penalties, but I was only indirectly involved in the monitoring of these, there was a unit inside Customer Service which monitored, and reported on all of these SLTs.

20. There were no SLTs relating to the management of software incidents or the production of code fixes.

<u>SOFTWARE SUPPORT CENTRE (SSC)</u>

21. As I state above at paragraph 7, I was the SSC Manager from 1997 to 2009.

22. The SSC's initial role was to provide 3rd line software support to Fujitsu-written software in the live estate, to accept incident calls from 2nd line support (SMC) in the PinICL (later Peak) systems. This involved analysing incidents, closing and returning those incidents that were not software related. For those that were software related, the SSC was to identify as closely as possible the root cause of the incident and pass the incident to the unit which could resolve it (usually in the development team), and thereafter to monitor the incident to completion.

23. The role of the SSC changed from this initial brief in a number of ways, under different Customer Service Directors.

24. Although I outline the changes that I can recall below, I regret that I cannot remember timescales, and only some of the reasons for the changes:

a. The SSC developed, supported, and maintained Peak for the reasons outlined in paragraph 14 above.

b. The SSC developed a visual monitoring tool to give early warning of any failures to servers and databases in the data centres and to give advance notice of possible incoming incidents. This was simply a support tool and, while it was not part of the Horizon system, it was subsequently made available to POL through the Service Management Portal.

c. The SSC were responsible for recovering any outstanding transactions which had been “stranded” on counters and not passed to the correspondence services in the data centres because the SSC occupied a secure area in Bracknell which connected to the live estate. I describe the process in more detail at paragraph 89 below.

d. The SSC were responsible for responding to ad-hoc data requests from POL—relayed through the Customer Service Management Support Team—for the reasons noted in paragraph 24(c) above.

e. The SSC developed, supported and maintained the KEL system.

f. The SSC developed the Service Management Portal—an initiative from the Customer Service Director at the relevant time, Dave Baldwin.

g. SSC staff reviewed technical documents relating to design, software development and support of new facilities and applications within Horizon because once the developed products were released to the live estate, the SSC would be responsible for supporting the code in those products. The SSC would provide written feedback (usually via me) to the document author.

h. SSC staff reviewed Change Proposal (**CP**) documents relating to changes in the functionality in the Horizon applications. As with technical documents, the SSC would be responsible for supporting any code that resulted from such CPs, and written feedback would be given (again, usually via myself) to the document author.

i. SSC staff designed and tested workarounds for reported issues on the live system.

j. SSC staff actioned corrections to data on the live system.

25. The SSC was/is the 3rd line software support unit. I was not involved in producing the processes for the other support units, and the extent of my understanding and recollection of these other units is as follows:

a. 1st line support was performed by HSH based in Stevenage. Their role was to respond to the call, identify the broad area of the issue and to check the KEL system. If the call was a hardware problem, they would pass the call to the engineering team; if the call was a network issue, to the network team. HSH would try to resolve the issue with the caller. If the call was believed to be a software issue, the call would be passed to the SMC for analysis.

b. 2nd line support was provided by the SMC, also based in Stevenage. In addition to receiving calls from HSH, the SMC was tasked with monitoring the state of the counters and the servers in the data centres using the Tivoli system. The SSC did not use the Tivoli software directly, but my understanding is that the system automatically reported on the state of the servers in the data centres, and the Tivoli software running on the counters would collate event messages and pass them to a data centre server. Event messages are entries in Windows NT (which was the operating system at the time) "event logs", which are included in all Windows systems. Windows operating systems and applications running on Windows write messages to the event logs which, as a result, are a major source of diagnostic information. There were an agreed set of targets with regard to SMC's relationship to the SSC—specifically "filtration" (i.e., the ratio of incidents which were inappropriately passed to the SSC). For example, the SMC had a target not to pass calls relating to hardware faults to the SSC. If the SMC passed 100 fault calls to the SSC, and 5 of these were subsequently closed as hardware faults, then the SMC's filtration rate would be 95%. The "End to End Support Process, Operational Level Agreement" dated 17 June 2003 (**End to End Support Process**) (FUJ00079897) sets out the categories of calls which should not be passed to each of the different support lines.

c. 3rd line support—software support—was provided by the SSC with similar filtration targets to 4th line support.

d. 4th line support was provided by the development team, which developed code fixes, or arranged for such fixes to be developed by external software suppliers.

26. These processes were the subject of Information Technology Infrastructure Library (**ITIL**) and British Standards Institution (**BSI**) audits. While I cannot recall specific audits, for BSI audits, I remember sitting with the auditor and responding to questions about processes, procedures, work instructions and relevant documentation, and the auditor would then spend time with one or more members of my team asking more questions. I also recall the SSC would receive observations and comments that would come out of the audits. I recall one ITIL audit where I had a long discussion with the auditor about the relationship between “incidents” and “problems" in ITIL terminology. The SSC passed this audit with no significant comments.

SSC staffing and roles

27. In 1997, when I joined, I recall that the SSC had 6 staff including contractors, and had only been recently set up in order to support the initial roll-out of Horizon to 10 Post Offices in the Stroud area. When I left in 2009 the number of staff was 25. I recall that at one point the staff level was close to 30, but I cannot recall when this was.

28. All of the people in the SSC reported to me—a flat structure. All but one, the SSC Coordinator, were tasked with diagnosing reported incidents in the live estate. When I left, the SSC technicians were graded the same as development

staff, ranging from DEV4 to DEV6, with DEV6 being the highest paid, most experienced and technically capable staff. Specifically, these were John Simpkins, Steve Parker, Anne Chambers, Patrick Carroll and Mark Wright.

29. All SSC technicians were expected know the Riposte product (from Escher). This was the software which ran on the counters and the correspondence servers in the data centres. EPOSS interfaced to Riposte on the counters. SSC technicians were also expected to have an overall understanding of the system structure, but they would then specialise in specific areas of Horizon—for example, Database, Agent and Counter—dependent upon their skillset on joining the team, the areas I felt the unit was short of staff, and their own wishes.

30. As a specialist in an area, the SSC technician would deal with incidents primarily, but not exclusively, in their area of specialty. For example, Counter specialists would concentrate on Riposte, EPOSS software and Escher Mails—any software running on the counters or in the correspondence servers. Other staff would concentrate on the systems which ran in the data centres.

31. The SSC Coordinator's role was mainly administrative; ensuring that out-of-hours call rotas were maintained, handling phone calls coming into the unit and ordering stationery. The SSC Coordinator also allocated incoming incidents on Peak as per my comments above.

32. During my time as SSC Manager, I recall reporting to Steven Muchow, Peter Burden, Carl Marx, David Baldwin, Naomi Elliot, Andy Hall and Wendy Warham. I cannot recall exactly when, and for how long, they were my managers.

33. I wrote job descriptions for Fujitsu's Human Resources team (**HR**) to use for external recruitment for the SSC. I can only vaguely remember the technical requirements for the SSC, but they would have included knowledge of at least two or three of Structured Query Language (**SQL**), AttributeGrammar, Java, C or C++ languages, and at least three years' technical support experience at the code level (meaning the ability to look at code to determine the cause of the incident).

34. In addition to the technical requirements that I specified, HR had additional requirements for SSC roles relating to security and financial checks, because we worked in a secure area, but I do not know the details of these.

35. Interviews with candidates for the SSC were done by me and one of the more senior SSC technicians, who prepared a set of technical questions which had to be answered correctly at the interview.

36. On joining the unit, new staff members were given a "joiners pack" which included a copy of their job description, SSC work instructions, and explanations of all the jargon and mnemonics. Since work instructions, jargon, and mnemonics changed on the Horizon systems, I would produce a new pack for each joiner.

37. New staff members were also allocated a "mentor" from the more senior SSC technicians. All new joiners were technically competent when we employed them. The mentor's purpose and responsibilities were to (a) train the new joiner on Riposte, (b) confirm the new joiner understood Riposte and the structure and functions of Horizon, (c) work with the new joiner and monitor their performance on incidents, and (d) generally "look after" them until they

understood the processes and systems. New joiners would initially have no access to the Horizon system. Using their judgment, the mentor would tell me when the new joiner was sufficiently trained to be allowed access to the live system and I would then request full access for them. I cannot recall specific examples of how long it took for new joiners to be sufficiently trained, but my recollection is that it usually took around 6 months.

38. Briefing of SSC staff on general matters relating to Horizon and Fujitsu were either done by senior management briefings, or by me, either in person, by email, or unit meetings. Such matters would include the status of the Horizon project, the Fujitsu company in general, and changes in management personnel. Technical information was available through the design, development and support documents held in Fujitsu's document system, which would be reviewed by SSC staff, and by staff simply talking to each other.

SSC reports

39. Reports on the operations of the SSC were prepared by me monthly and sent to my manager. The format varied depending on the requirements of my manager. For most of the time that I was SSC Manager, my immediate manager was the Customer Service Director, but there were occasions on which I reported to someone who then reported to the Customer Service Director.

40. The purpose of the SSC monthly reports was to inform my manager on the operation of the unit. I recall that the report always included figures for the volume of calls coming into the SSC, the number of calls closed, as well as showing categories and filtration rates between the SMC and the SSC, and

between the SSC and development team. There was always a section relating to any major incidents reported in the system (those incidents which had been forwarded to the SSC with a high priority). Later reports would also include details of staff time and activity, any ad-hoc data requests made by POL and any transaction recovery actions which had been taken. Where relevant, information in the SSC monthly reports would feed into Problem Management meetings and Service Reviews with POL.

41. The SSC did not undertake trend analysis to determine whether the same issues were recurring, as this was the responsibility of other Customer Service staff based on data supplied by the HSH and SMC (i.e., the calls in Powerhelp). The SSC were only supposed to receive the first instance of a new software issue. If there were multiple calls, there was a facility for the HSH/SMC to identify those calls onto the Peak system.

42. If the SSC recognised that a particular problem could have implications for multiple branches, this was added to the Peak and the KEL. It is important to note that problems which occurred in overnight processing sometimes had the potential to affect all Post Office branches, but not every potentially affected branch would be listed on the Peak.

Service Management Portal

43. The Service Management Portal (**SMP**) was an initiative proposed by the then Customer Service Director (Dave Baldwin), to be written by the SSC as something completely separate from the live estate and the formal development of Horizon. It was created in about 2006, and it was a prototype to demonstrate the ways in which Fujitsu could display data of interest to POL.

44. The development was to be an intranet system accessible by POL management and Post Office Account staff which would provide a variety of functions. The functions that I can remember were reporting against hardware call SLTs, reporting on network reliability, real-time reporting on some system functions, and a function that would show the nearest working Post Office branch in the event of network failure causing one or more branches to cease trading. As noted in section 4 of the “Service Management Portal User Guide” dated 22 December 2005 (**SMP User Guide**) (FUJ00142216), the real-time reporting was a red/amber/green representation of the state of a number of system functions, including Alliance and Leicester Network Banking, overall failure count on Network Banking transactions, Transaction Enquiry Service servers and EPAY connections for E-Top Ups. In addition, there was a map of all Post Offices which were not communicating, with subsets for VIP Post Offices and Post Offices that were reliant on satellite communications. POL could also check on the current state of an individual Post Office. The data which was used to provide the information was detailed on the SMP.

45. I cannot recall the names of individuals who had access to the SMP. I arranged for Fujitsu and POL staff to be given access but I would not deal directly with the individuals being given access. For example, POL would supply me a list of POL staff to be given access, and I would add these names to the SMP system and provide POL a list of usernames and passwords.

46. Most of the SMP system was written by me, with assistance from SSC technicians. Data for the system came from daily extractions from Peak, Powerhelp and Tivoli.

47. Access to the SMP system was restricted to some POL management staff whose roles I did not know (I was simply provided with names, so that I could set up usernames and passwords) and Customer Service staff. Through the SMP, it was possible to access some underlying Powerhelp calls which would include updates to relevant Peaks.

48. My recollection is that the SMP system had additions made over several years, including major incident management, reporting against SLTs to the Service Review Board, Operational Business Change and Operational Change Proposal (**OCP**) procedures, but was not often used by POL management, and (from comments relayed to me by Customer Service management) showed every sign of withering to nothing by the time I left in 2009.

49. As part of my work on the SMP, I prepared documents to support its use. I wrote these documents at a time when it was believed that the SMP would be in regular use:

   a. SMP User Guide (FUJ00142216) for Fujitsu and POL staff using the SMP.

   b. "Service Management Portal Support Guide" dated 29 August 2007 (FUJ00142217), which was a detailed technical support guide, so that SSC staff members would be able to support the SMP in my absence.

   c. "Service Management Portal High Level Design" dated 19 July 2007 (FUJ00142218), a design document using the standard format for design documents at the time.

Recollections of my time in the SSC

50. I remember on my first day thinking that running a software support team which, at that time, did not have adequate access to the system to gather evidence, nor the Fujitsu-written source code that we were supporting, was going to be an impossible job. It left me wondering what on earth I had taken on. It also came with a very long “to do list”.

51. This situation did improve rapidly. The SSC was given greater (but not full) access to the system—parts of the system were still not accessible, for example, the audit server. The SSC was also given read access to the source code. The relationships between the different support units (i.e., the HSH, SMC, SSC and development teams) were defined, additional staff were recruited and we moved to a secure location in Bracknell. We also developed a specification of the equipment required for a test rig specifically for SSC use, which the SSC would use to recreate problems reported on Horizon. Over time, I was able to complete all the items on my “to do list”.

52. Overall, I suspect that, like everyone else in every other job, there were some good days and some bad days. I remember thinking that I did a good job of treating my staff with respect and managing the team, and getting the software problems with the system managed properly.

53. I believe that the SSC provided a professional and competent service, both to POL and to Fujitsu. The unit regularly hit or exceeded the targets which we were set, developed and maintained support tools for the SSC and for other support teams, and provided a service to POL for management information

which was beyond the scope of the contract (for example, by producing ad hoc reports and developing the SMP).

54. The SSC staff, for the most part, seemed to me to be happy in their work and staff turnover was low. This meant the team's performance was consistent, there were fewer new joiners requiring training, information could flow freely between team members and incidents were therefore resolved quickly.

55. As with any job, there were bad times when incident rates were high, and staff worked long hours to resolve incidents or times when staff were being called in to the office overnight to resolve incidents with the data centre systems.

56. I cannot remember specific technical issues, however I can recall one instance where myself, an SSC technician and a member of the Belfast Operations Centre support staff (**BOC Personnel**) were in Bracknell throughout the night trying to resolve a problem with overnight processing which would have had a major impact on the following days' business for Post Office branches. I remember the problem was resolved in time, but as I have mentioned above, I do not recall the exact nature of the incident, or how it was resolved.

57. On a number of occasions, problems with overnight processing could cause SSC technicians to be called into the office at Bracknell. If the SSC technician felt that the incident was likely to cause impact on POL, the SSC technician could contact me, and I would go to the office. Due to the time that has passed, I cannot recall specific occurrences, dates, or the incidents that caused them.

SSC's relationships with other units

58. Since the SSC was the 3rd line software support unit, incidents were reported to the SSC by the SMC (2nd line support unit). There was, therefore, no direct relationship between the SSC and the HSH (1st line support unit). Nor was there a direct relationship between the SSC and the NBSC.

59. The SSC's "supplier" of incidents arising from postmaster calls was the SMC, and incidents were not supplied directly from HSH or NBSC. Therefore, the SSC had direct interfaces and relationships with SMC and the development teams (4th line support). Ultimately, SSC, SMC and HSH were the responsibility of the Customer Service Director.

60. The relationship between the SSC and SMC was generally cordial, although I know there were concerns at times about SMC's ability to correctly filter calls, and the impact this was having on the SSC (i.e, an increased volume of incidents being raised that did not require intervention from the SSC or development teams). There were also times when SSC staff felt that important system errors in the data centres were being missed by SMC, leading to pressure on SSC staff.

61. Where concerns were raised, the SSC and SMC would have meetings, and I recall meetings with SMC managers to discuss these issues. Initially this involved me specifying Service Level Agreements (**SLAs**) to the SMC to identify in more detail what the SSC required from the SMC, monitoring the SMC's performance against those targets, and then discussing anomalies to see if there were ways in which we could rectify them. I recall that one specific area of concern was the SMC's ability to monitor Tivoli events correctly, and

that part of this was the way that Tivoli was configured. This was referred to as an "event storm", and it was the responsibility of the HSH/SMC to monitor these, which is detailed in the End to End Support Process (FUJ00079897).

62. As discussed in the section relating to the SSC's position in the support hierarchy, the SMC were tasked with filtering all calls except software bugs. Since the incident was going to be passed to the SSC, it is natural and correct that the SMC staff member raise a KEL, and also natural that they would believe it (through, in my experience, a process of elimination) to be a software bug (rather than, for example, user error) and record it as such on the incident or problem management systems.

63. I have only vague recollections of the interface between the SSC and the MSU. The MSU would pass to the SSC requests from POL for ad-hoc data, and monitored and reported to POL on all the contractual SLTs. I also recall a process in which the MSU would receive information about mismatches in accounts and would then raise a Peak for SSC staff to investigate.

64. The working relationship between SSC and development teams (4th line support) worked well. SSC staff were always at liberty to contact development staff to discuss incidents. Generally, this would involve senior SSC technicians. One SSC staff member, Patrick Carroll, was placed on long-term loan to development, tasked with developing the server that would provide the SSC with access to the live systems at HNGX.

The proportion of incidents referred to the SSC

65. The SSC did not receive incidents direct from the HSH or NBSC, only from the SMC. I remember agreeing and then documenting a set of targets by which

the SMC and SSC would be judged by other lines of support and which allowed Support Units to monitor their performance relative to expectations, which are detailed in the End to End Support Process (FUJ00079897). This document set a target on the SMC to only pass to the SSC the first instances of new software bugs. That is to say, no calls which were subsequently closed as user error, network error, hardware, documentation, duplicate calls and other categories documented in the End to End Support Process (FUJ00079897).

66. Initially the number of incidents passed to the SSC was very high and the “filtration” from the SMC was inadequate, which could result in SSC staff being overloaded with calls which were not software-related. Measures were put in place to change this. I remember going to Stevenage on several occasions to give presentations on the system structure, and there were also some secondments from the SMC to the SSC. SSC-developed tools such as the KEL system were also introduced, and SMC were granted access and encouraged to create KELs. Over time the filtration rate from the SMC improved consistently, meaning the SSC was adequately staffed to deal with incoming incidents.

Major incidents

67. At the request of the Inquiry, I have considered the “Horizon Service Desk Joint Working Document” dated 4 September 2008 (FUJ00080096). The document does not appear to mention the SSC and relates to the HNGX, which had just gone live when I left Fujitsu. As far as I can tell, the document sets out the processes to be followed by helpdesks.

68. As I specify above at paragraph 15, incidents were reported to the SSC by the SMC (2nd line support). Major incidents (i.e., "A" priority) which were being sent from SMC to SSC would be preceded by a phone call alert from SMC to SSC.

69. I reported on any incidents which were major—i.e., any incidents which were "A" or "B" priority in the SSC monthly report. In general, major issues were those that had the potential to affect a number of Post Offices, or which had a significant impact on the functioning of servers in the data centres and therefore were reported by the Tivoli monitoring software. The SMC were responsible for the monitoring of Tivoli, and therefore the incidents would be raised by them.

Prioritising incidents

70. The input that I had to the prioritisation of calls in HSH was limited to software calls. Although my name is shown as author of the "Call Enquiry Matrix and Incident Prioritisation – Software" specification dated 23 April 2007 (FUJ00080499), I have no recollection of this document, and I must have had significant input from elsewhere, because I never used the Powerhelp system and would not have known the "Cause Codes" or "Repair Codes" used in the document.

SSC resources

71. The rate at which incidents were presented to the SSC fluctuated greatly. This could be due to, for example, reference data changes, new functionality being introduced to the system, software releases. All of these had the ability to increase the number of incidents being reported to the SSC. Sometimes I felt that I did not have enough time or resources, at other times, overtime claims

were very low, and the incident rates were also low, and I had all the resource that I needed.

72. I was concerned whenever call rates rose, or whenever the SMC did not hit their “filtration” targets, that my staff would be overstretched. I recall reporting to my management about those concerns in my monthly reports.

73. That having been said, the SSC did not get overwhelmed by incidents, and the number of incidents which were resolved kept pace with the number being reported. Furthermore, the SSC staff also had sufficient time to respond to ad-hoc requests for information from POL and from Customer Service, and to develop tools to help in their work. So overall, I believe that we did have sufficient resources and time, including staff, to investigate reported incidents.

74. At the Inquiry’s request, I have considered the following documents: POL00004074, POL00004075 and POL00000678. With regard to SSC staff members raising with me issues over having sufficient time or resources to investigate potential problems. I do not recall specific instances, but there were occasions when on-call staff had been called in to the office for major issues with the central systems when we all knew that the problem could have an impact on the live estate. For example, a number of Post Offices not being able to trade the following day until the problems were resolved. These were obviously time-critical problems, and we always wished that we had more time.

75. There were also occasions in which SSC staff needed help from development staff overnight to understand a particular issue. In these circumstances, I felt it part of my job to call development managers and request their staff’s assistance, even though they were not on-call.

76. With high priority incidents, there was always a degree of “pressure” to establish a root cause for an incident, and, if possible, produce a workaround, or at least mitigate its impact. Under these circumstances, SSC technicians may well have felt that they wanted more time, and more resource to resolve the incidents, and may well have told me so. The SSC technicians working on the problem could have access to resources that they needed to resolve the problem, and during my time as SSC Manager, I do not recall any occasions where I denied requests for additional resources, or any occasions where my requests for additional resources were denied.

ESCHER AND RIPOSTE

77. Incidents relating to third party software were handled in the same way as any potential software error. The SSC would thoroughly analyse the evidence obtained from Horizon in order to establish the root cause. The only difference in the process would be that the SSC would not have access to the source code. However, it was possible to establish that the root cause was related to third party software by looking at the points of interaction between the Horizon code and the third party supplier’s code.

78. My recollection of the process is that the Peak would be transferred to the development unit responsible for the support contract with the third party supplier and that the development team would manage the interface with the supplier.

79. This was certainly the case with Escher with regard to potential defects in the Riposte system. The support contract with Escher mandated that only certain

people within Pathway (and later Fujitsu) were permitted to communicate direct with Escher.

80. Since, at the time that the contract was put in place, Horizon was a development project with no support teams, the list of contacts included only development and managerial roles.

81. I remember that there were software errors in Riposte, although I do not recall the specific issues. However, I have watched the oral evidence provided by Stephen Muchow and John Simpkins to the Inquiry on YouTube, which indicates that there were more errors than I first recalled.

82. Handling the interface between Fujitsu and Escher was outside my knowledge, but from the point of view of the SSC, it took longer to resolve incidents where external suppliers were involved.

83. Since I was not included in the list of contacts who had a direct relationship with Escher, I cannot comment on Fujitsu's working relationship with them. I also have no knowledge of the relationship between the development team and Escher.

PROCEDURE FOR IDENTIFYING AND RECTIFYING BUGS

Recollection of bugs

84. In the Request, the Inquiry has asked me to set out my recollection of the identification and rectification of:

   a. the bugs identified in *Bates and others v. Post Office Limited (No. 6) "Horizon Issues"* [2019] EWHC 3408 (QB), having regard to Appendix 1 (the **Technical Appendix**) and Appendix 2 (**Summary of Bugs**) of the judgment, save for bugs 16, 17, 21, 22 and 29; and

b. any other bugs that had the potential to cause apparent discrepancies or shortfalls in branch accounts, or that could undermine the reliability of Horizon to accurately process and record transactions.

85. As I explain above, I was SSC Manager from 1997 until 2009. HNGX did not go live until the year after I had left Fujitsu, and I do not recall being involved with Peaks relating to HNGX. Many of the bugs set out in the Technical Appendix relating to HNGX appear to have been identified or reported after I left Fujitsu.

86. I believe that Steve Parker's evidence to the court, documented in POL00004075, explains that during the period January 2001 to December 2014, 27,005 incidents were passed to the SSC at an average of 563 per month. As I have been away from this environment for 13 years, I regret to say that I have no recollection of any specific Peaks, PinICLs or KELs, including those that have been referenced in the Technical Appendix and Summary of Bugs. I have also been shown Peaks containing entries made by me, which are said to relate to the bugs noted in paragraph 84(a) above, and I do not have any specific recollections regarding these Peaks.

87. In relation to bug "12. Counter-replacement Issues" in the Technical Appendix, I do remember there were occasions in which a counter replacement caused incidents which were reported to the SSC. I also remember that processes were put in place with the MSU for SSC to retrieve any overwritten transactions so that MSU could report on these to POL.

88. The Riposte software on a counter should always replicate transactions to other counters in the branch. In the case of a single-counter branch, the counter had a mirror disc. Therefore, if a branch was transitioning from multiple counters to a single counter, the remaining single counter should have had a mirror. If it did not, then this was a failure of process. My recollection is that Riposte messages and transactions could be treated the same (although I do not know if there is a technical difference between them), and the Riposte message store was the collection of Riposte transactions or messages held on a counter, replicated to other counters in the same Post Office branch, and replicated to the correspondence servers in the data centres.

89. As mentioned at paragraph 24(c), I know that there was a process used by engineers which was used to recover “stranded” transactions from counters at Post Office branches. When this occurred, the engineering team would attend the Post Office branch to recover the transactions at the branch. If a counter would not connect to the local LAN, the engineers would use a data recovery laptop, connected to the counter to extract data in the Riposte message store. The exact nature of the process followed by the engineering team, and the build of the laptop is not known to me. If this process failed, and the SSC were able to liaise with the network team to make reconnections, then transactions could be recovered. As a last resort, if this process failed, the affected counters would be taken from the branch and returned to the SSC’s secure area in Bracknell which connected to the live estate. I cannot comment on the extent to which stranded transactions could lead to discrepancies in branch accounts, but I presume they would have a financial impact somewhere in the system.

Fujitsu's process upon identifying bugs

90. The steps taken to identify bugs and discrepancies in branch accounts were no different, from the SSC point of view to the steps taken to identify any potential bug in any part of the system, namely some, or all of the following:

a. Gather the evidence for the reported incident

b. Analyse the data from Horizon to identify the source of the problem

c. Attempt to recreate the problem using reference equipment

d. Analyse the source code (as noted in paragraph 77 above, this step could not be taken in relation to third party software)

e. If the problem could be fixed by a workaround, then develop and test that workaround

f. If the problem required a code fix, then attach the evidence to the Peak and pass to the relevant development team

91. If it was recognised by the SSC that an issue could affect branch accounts, this would be stated on the relevant Peak. There were problem and major incident processes in place, but do not remember them, and these processes were run outside of the SSC, which is noted in the "POA Customer Service Problem Management Process" dated 29 July 2005 (**Problem Management Process**) (FUJ00079953). The only difference that I can remember in relation to the SSC's process for dealing with a potential bug that could impact branch accounts and any other potential bug would be the parts of the system from which the SSC would gather evidence.

Releases and release management

92. When a bug was identified, either by the SSC or 4th line support staff working with the SSC, a developer in 4th line support would outline the expected time that would be required to develop a code fix.

93. At this point the Release Management process would come into effect. As part of this process, there were weekly meetings between the Live System Test team (**LST**) (which was co-located with the SSC in Bracknell), release management staff, development staff and SSC. I usually attended these meetings.

94. The decision as to the timescales to fix any bug would have been taken by the release management forum, and would be dependent on a number of factors, which would include:

   a. Potential impact of the bug to Post Office branches (including postmasters)

   b. Length of time required to produce a code fix

   c. Length of time to test the fix

   d. The equipment needed to test the fix

   e. Priority of the fix in relation to other fixes currently in process

   f. Potential risks of implementing a fix

   g. Availability and effectiveness of any mitigating factors / workarounds.

95. The release management forum was an internal Fujitsu meeting. Input was sought from POL regarding the business impact of specific incidents, which would be relayed to the release management forum by one of the attendees. From this discussion would come a schedule for the production, testing and release to the live estate of any fixes.

96. The release and implementation of all code fixes to the live estate was the responsibility of the release management team. My recollection of the process is that any fixes required to be applied to Horizon's code would go through the release management process, and these code fixes would be implemented using Tivoli software.

97. There were different types of releases: major releases and interim maintenance releases. Major releases were fixes to known bugs plus new functionality, for example, a change of data centre, while interim releases were bug fixes that could not wait until a major release because of business impacts. I recall POL was involved in the release process, certainly in the early stages regarding the content of releases, but I cannot recall exactly how the process was managed. For major releases, POL was very involved, to the extent that POL staff would be on site in the SSC secure area in Bracknell monitoring the progression on the release deployment. I can recall attending one major release with John Bruce from POL, but I cannot remember the details.

Code fixes and workarounds

98. Whenever a code fix was to be sent to the live estate to rectify a bug, it would be tested by the LST. The LST used a test rig with "live keys" in order to make it as close as possible to the systems used in the live estate. The LST and SSC

shared the use of this test rig and therefore, whenever SSC staff were creating rectification for problems, or trying to recreate issues in a controlled environment, this is where such testing would take place.

99. If a code fix was unsuccessful, Peaks would be raised based on the symptoms being experienced. Some fixes could be regressed, which means the fix could be removed from the live estate and replaced by the original state (i.e., the code that was in place before). If a code fix could not be regressed, there would need to be a fix for the fix, which would be handled in the same way as any other incident.

100. Where workarounds were produced, they would be documented on the relevant Peak, and the steps necessary to apply the workaround would be documented in instructions to SSC staff. If the workaround was likely to be used on a consistent basis, scripts would be produced in cooperation with development staff.

101. Test rigs outside the LST did not use “live keys” and so were not identical to the live system. Workarounds would be tested on the test rig which most closely aligned with the live estate. I cannot recall the processes by which POL was involved in the testing of code fixes.

102. Workarounds would be implemented for any bug based on a number of criteria, the primary one being the impact of the bug to Post Office, by which I mean the whole business, including POL and postmasters (to the SSC they were all “the customer”). Other criteria would be discussed at the release management meetings. My recollections of this process are detailed above at paragraph 94.

103. A workaround could be offered to an identified bug in place of a code fix for a number of reasons. For example, if the code fix would take a long time to produce, if a code fix was impossible to test, or if the exact root cause of the bug could not be identified and therefore the code responsible for the bug could not be identified. As noted above, discussions concerning these issues would take place at the release management forum and the decisions taken there. A workaround could be specific to one incident, but it could also apply to other incidents with the same, or similar symptoms. The nature of the workaround could also differ depending on the nature of the problem.

104. If a rectification in the form of a workaround was possible, then the SSC would use the test rig to test the workaround.

Sharing information

105. There were no procedures or work instructions of which I was aware that restricted the flow of information about any workaround or potential bug anywhere in Horizon.

106. SSC staff would frequently discuss any reported issue at a Post Office branch with the postmaster there and would discuss any workaround or potential bug with the development staff responsible for the code. As far as I can recall, there were no instructions passed to me, nor was any pressure applied to me restricting to whom I could talk about workarounds, potential bugs or perceived failings in Horizon.

107. When incidents were closed, this would be communicated to the postmaster who raised the incident by the HSH/SMC. In cases where the SSC was communicating with a postmaster about an incident, SSC staff would

sometimes agree closure of the incident with the postmaster. If a workaround was being applied, POL would sometimes liaise with the postmaster as to when the workaround was to take place—for example, if messages needed to be inserted to the counter message store. As I recall, these types of workaround required liaison between Fujitsu, the postmaster and POL, because (a) the postmaster would have to have the Post Office branch open (otherwise transactions would appear after end-of-day processing and cause failures), (b) Post Office branch staff would have to log out of their counters (otherwise the Riposte sequence number would mismatch and cause error), and (c) POL would also be asked to confirm that the inserted transaction had been successful. However, workarounds that were applied to data centre systems were not always agreed, or discussed with POL.

108. There were processes in place detailing the interface levels for normal communication between POL management and Fujitsu management—Problem Managers in each organization would communicate with Problem Managers at the other, Directors with Directors, and so on. I believe that the documentation for this was the Problem Management Process (FUJ00079953). I do not recall being involved in this process to a significant degree. I was occasionally involved in some conference calls with POL relating to problems or major incidents, but these were rare exceptions.

109. As part of the SSC's processes, communication with POL management would normally go through the Business Support or Management Support Units within Customer Service rather than direct by SSC staff.

110. I do not believe that any of these procedures or practices imposed any restriction or pressure on myself or my staff not to pass information to POL or within Fujitsu. I cannot recall any instances where either myself or my staff were restricted or pressured to not pass information to POL. There were documented "lines of communication" between POL and Customer Service as outlined in paragraphs 108 and 109.

111. There were prohibitions on the viewing of diagnostic data from the system outside of the SSC secure area. It was possible, particularly after the introduction of banking applications, that the diagnostic data could contain "personal data" (which I believe was defined in relevant data protection legislation). Therefore, this data would be held in secure servers on the live system and the data could only be viewed using the purpose-built SSC PCs connected to that live estate. This meant that, in the event that a Peak was passed to development staff, they would be allowed access to the SSC secure area by the SSC staff member who had been allocated the Peak.

Notes of prayers

112. At the Inquiry's request, I have considered the email from Lionel Higman to myself and others dated 18 July 2005 (FUJ00086334) and the "Note of Prayers" dated 18 July 2005 attachment to the email (FUJ00086335). I cannot remember the exact purpose of the "prayers" meetings, although I have a vague recollection that they were a daily meeting to discuss development issues relating to upcoming releases. I note that a number of Customer Service managers were included on the distribution list for the Note of Prayers meeting on 18 July 2005, including testing, release and support managers.

Peak PC0145617

113. At the Inquiry’s request, I have considered Peak PC0145617 (FUJ00086828). For the reasons I have explained at paragraphs 85 and 86 above, I cannot recall the details of any specific Peaks. Reviewing the details of Peak PC0145617 has not prompted any memory of the incident.

114. Looking at the Peak, the issue, as reported by the Postmaster, appears to be that the screen would “freeze” during a transaction, forcing the Postmaster to reboot the counter. There is no indication from the Peak that this would have any impact on branch accounts. I believe that my reasons for stating that Fujitsu was unlikely to get a fix from Escher, and that it was unlikely Fujitsu would implement such a fix even if it were provided by Escher, are contained within the Peak. Fujitsu’s development, network and SSC teams, and Escher, could not identify the root cause of the problem, which appeared to lay somewhere between Escher code and network issues. Therefore, there was no realistic expectation of a code fix from any source.

115. Again looking at the call, it appears that it was not possible to recreate the bug in a test environment, there was also no realistic expectation of being able to test any code fix supplied from any source. The development team’s suggestion was that any potential code fix would be likely to cause more problems than it solved, and a workaround was available (documented in the call as a change to the relevant Post Office branch’s network type), which was the solution that I recommended. The underlying problem was a combination of a Riposte process error and a network failure occurring simultaneously. This only happened on the ISDN network, and the effect of the workaround was to switch

the branch to a different and more expensive network (ADSL) on which the issue did not occur.

116. By recommending in the call that "no attempt be made to fix these problems", I was recommending that no code fix be written. The call records my recommendation that Fujitsu implement network changes which had been shown to resolve the issue without requiring a code fix—even though this workaround would have a cost implication to Fujitsu as the ADSL network was more expensive.

117. I wish to stress that I do not recall the details of this incident and my explanation above at paragraphs 113 to 116 is based on my interpretation of the Peak, 16 years after the event.

REMOTE ACCESS

Remote access and my role as SSC Manager

118. In responding to the Inquiry's questions on the topic of remote access, I wish to stress that at no time did I personally use remote access to any part of Legacy Horizon or HNGX. I never requested access, nor did I ever want it, not being sufficiently technical. I was a manager of SSC support staff, and therefore was not sufficiently technically trained in Riposte or any other part of the system to provide technical support. I did not need access to either the Legacy Horizon or the HNGX systems. My knowledge of remote access is not as detailed or comprehensive as the SSC technicians who I managed and who did use remote access to provide software support.

119. It is clear from the Peaks that I have been shown—for example, Peak PC0143500 (FUJ00120588)—that the use of remote access could affect

Post Office branch accounts. Transactions were only inserted to make corrections to previous erroneous transactions, and therefore those transactions would be expected to impact the branch accounts. The exact impact of this use of the SSC's is beyond my technical knowledge. I do know that the SSC PCs and later laptops were "fixed build" with toolsets and audit requirements agreed between the SSC, Security Architects and others.

SSC access rights

120. SSC staff members with access to the SSC PCs had access to Horizon, including live Post Office branch data, from the secure area in Bracknell. The SSC PCs were located in the secure area. Only SSC and LST staff, and at one point Release Management, had access to the secure area. In order to use the SSC PCs, it was necessary to have log-in credentials and "key-cards" which generated one-time passwords for dual factor authentication. This was restricted to SSC technical staff only—this did not include the SSC Coordinator, new joiners, LST or Release Management. For example, I did not have access to the SSC PCs. During times of major releases, BOC Personnel would use SSC PCs to perform the release deployment. For this activity, they would use their own secure ID 2-factor authentication.

121. The facilities to do all functions relating to Horizon were built into the SSC PCs, and I believe the nature and extent of the SSC staff member's access depended on their "role"—a technical term—which would distinguish between types of access on login to systems. I do not recall the exact details of these roles or their access, so I am unable to comment further on the extent to which this access extended to the branch accounts.

122. I do recall that no SSC staff members, nor indeed anyone else, could change or delete transaction data in the counters. Transactions in Riposte were immutable—they could not be changed or deleted.

123. If a postmaster made a mistake, a transaction could be "reversed" (by inserting a "reversal" or "corrective" transaction) but it could not be deleted. There were processes by which SSC staff could, under instruction or approval from POL and with assistance from the postmaster, insert corrective transactions, and I recall that there were processes in place to control this rare occurrence, involving dual-person sign-off on the Peak and approved OCP requests for the SSC to do the work, which I believe had to be approved by POL as well as Customer Service. An example of this process is OCP 21918, titled "Insert Corrective Transactions at Branch 382137" dated 2 March 2009 (**OCP 21918**) (FUJ00084131). My recollection is that the process was technically complex and could only be done in agreement with the postmaster and was extremely rare.

124. As documented in "Secure Support System Outline Design" dated 2 August 2002 (**System Outline Design**) (FUJ00088036), prior to the introduction of Network Banking, the SSC could only do the activity with cooperation from counter staff. Once Network Banking was in place, then Secure Shell (**SSH**) software was implemented, and everything that the SSC did had a full audit trail.

125. Not all SSC staff had such access. As I note at paragraph 37 above, new staff joining the unit were allocated a "mentor" from the experienced SSC staff. Only when the mentor felt that they were technically ready were they allowed access

and I do not recall anyone being allowed the access within the first six months of joining the unit.

126. As outlined above at paragraph 34, HR had specific vetting processes for Fujitsu staff working on the Post Office Account, and additional vetting processes for SSC staff. If I was ever told what those additional vetting requirements were, I have forgotten them. I do recall that one person who I interviewed for a role in the SSC was subsequently rejected by HR for having a County Court judgment against them which was undisclosed.

Remote access procedures

127. At the request of the Inquiry, I have considered the design document titled “Host BRDB Transaction Correction Tool Low Level Design” dated 13 November 2007 (**Design Document**) (FUJ00084135). The Design Document is for a tool to correct transactions on the central database (**Transaction Correction Tool**), which is intended for SSC use. The document and the Transaction Correction Tool itself is only relevant to HNGX.

128. My involvement in this process was to ensure that the tool was produced and delivered to the SSC for HNGX. I left Fujitsu before HNGX was implemented and therefore have no knowledge concerning the use of the Transaction Correction Tool.

129. During the period Legacy Horizon was in operation, the SSC could only insert transactions into the counters—and therefore Post Office branch account data—via Riposte. There was also a separate tool, the TIP Repair tool, which could correct data that had been sent to POL via a data centre system. My

recollection is that this tool generated separate correction files to POL, and not all of these correction files would have had an impact on branch account data.

130. In HNGX, Riposte was no longer used in Horizon, and therefore the function needed to be transferred to the central database. As I stated in paragraph 122 above, transactions in Riposte could not be changed or deleted.

131. Although I cannot remember the technical details of the design of the Transaction Correction Tool, it is apparent from the Design Document (FUJ00084135) that the use of the tool only enables the insertion of a transaction, and its use is audited through the logfile, which is a part of the standard Oracle product.

132. There would certainly have been restrictions placed on the use of the Transaction Correction Tool, and as suggested in the Design Document, the tool was restricted to a few SSC staff.

133. At the request of the Inquiry, I have also considered an email exchange between myself and Simon Ajina from November 2008 to January 2009 (FUJ00086866). At that time, Simon Ajina was responsible for ensuring that the Customer Service requirements for HNGX development were being met.

134. As part of the process for design and development of HNGX, a number of requirements from the SSC were documented that related to tools specifically for SSC use (for example, documented event point in the code). The email exchange between myself and Simon Ajina (FUJ00086866) relates to SSC requirements to access the live system elements in HNGX, and not Legacy Horizon.

135. I do not recall the full details of the system checks put in place to control remote access. I do recall that Horizon's processes involved using only "defined-build" (or "fixed build") PCs and latterly for out-of-hours call-out laptops (the SSC build specification was held as a document in the Fujitsu document system and would have been approved by development, support, security and senior managers). I remember Glenn Stevens (who has sadly died) from design/development being the SSC's interface. I also recall that the process for using these PCs involved a two-stage login process involving a one-time password generator, and that the PCs were connected to a dedicated, secure, LAN and that links were encrypted.

136. My role would have been to review and approve the documents relating to the SSC PC build. Whenever there was to be any correction to any data, the process involved the raising of an Operational Change Proposal (**OCP**), which usually had a number of signatories. I cannot recall the full list of possible signatories, but I was certainly one.

The System Outline Design

137. At the request of the Inquiry, I have considered the System Outline Design (FUJ00088036). I do not know what the Tivoli remote console was and I do not recall SSC staff using Tivoli "Remote Console". The System Outline Design refers to support tools for all support units, including the SSC. As I have mentioned above at paragraph 25(b), Tivoli software was used by the SMC and SSC did not use the software directly. Tivoli monitored servers in the Horizon system and it generated alerts to indicate the possibility of errors, which Tivoli would pick up from operating system events logs. As I understand it, Tivoli was

mainly accessed by the operating systems on the servers, primarily Windows NT. The operating systems were not supported by the SSC, which only support code written or implemented by Fujitsu.

138. BOC Personnel, which I mention at paragraphs 56 and 120 above, supported the operating systems and databases. These staff were based in Belfast. I do not know what tools they used to support those parts of the Horizon system.

139. At the time that the System Outline Design was produced, access to the live estate was not fully audited. Audit trails did exist, and included recording of staff login/logout on SSC PCs and SSC servers in the data centres.

140. What was not directly auditable in the early stages of Horizon was exactly what the SSC staff had typed when logged into the SSC PCs and SSC servers, although the logins themselves were auditable. Other audit trails were manual, through the use of OCPs or updates to the Peak system. If a transaction had been inserted into a message store, this would have also been visible in the message store.

141. The purpose of the System Outline Design seems to be to specify a toolset for different support units to enable them to continue to support the systems, and to be fully auditable. The System Outline Design resulted in the use of SSH software, which was fully auditable—I believe via the audit servers, which were not accessible by the SSC.

142. SSC access to the live system from the secure area in Bracknell was not automatically audited in the early stages of Horizon because at the time, the only software that could provide the access necessary to support the Horizon

system was called RClient. RClient was a Microsoft utility which did not support the audit of specific keystrokes. The operating systems—Windows NT at the time—logged all Login/Logout events, so it could be determined when any SSC staff accessed the live system and when, but exactly what they had done could not.

143. After 2002, SSH was implemented on all elements of the Horizon solution, and exact keystrokes could be audited.

Operational Change Proposal 21918

144. At the request of the Inquiry, I have considered OCP 21918 (FUJ00084131) and the email from Matthew Lenton to Jonathan Gribben dated 25 June 2019 (FUJ00087871).

145. I have no recollection of the specific error relating to this OCP. However, it is apparent from OCP 21918 (FUJ00084131) that POL were aware that a corrective transaction was being inserted and had approved it (Julie Edgeley of POL is quoted as having agreed to the change and Gary Blackburn of POL is copied), and Gaby Reynolds of Fujitsu records that POL signoff has been attached to the OCP. The document also contains a note from Julie Edgeley to Anne Chambers informing her that the manager at the Post Office branch (Wendy) has also been informed.

146. I have no recollection of the term APPSUP being used while I was SSC Manager.

CONDUCT OF PROSECUTIONS

147. I was not involved in the case of *POL v Lee Castleton*, and I did not know of this case before receiving the Request.

148. Anne Chambers was one of the most experienced and technically competent of the SSC staff during my time as SSC Manager. As such she reported directly to me.

149. Of the staff who were on the highest grade within the unit, Ms Chambers was the “lead” on counter software (including, for example, Riposte and EPOSS). My relationship with her was always positive and professional and I do not recall any negative comments that I wrote about her on my annual reviews of her performance in which, to my recollection, she always scored highly.

150. I always found Ms Chambers to be dedicated to finding and resolving incidents, and thoroughly professional.

151. I was aware at the relevant time that Ms Chambers was asked to give evidence at the prosecution of a postmaster. This was the only time that I am aware an SSC staff member gave evidence at such a case and it was done despite my strong objections, which I explain below.

152. Fujitsu’s security team, which sat within Customer Service, were responsible for the “Litigation Support” service. My understanding is that the process would generally involve the security team obtaining evidence for any litigation from the audit server. The SSC did not support this server and did not have access to it.

153. In this particular case, the person at Fujitsu who was originally responsible / going to give evidence at court declined to go. I cannot recall who this person was or why they declined. My recollection is that Brian Pinder was the Customer Service manager of the security team at the time, and I believe it would have been his responsibility to perform this task within his team.

154. I was instructed by the Director of Customer Services at the time, whose name I cannot recall, to detail someone from the SSC to go to court to explain the workings of the message store. I objected strongly that nobody in the SSC had any experience of courts, or was legally trained. I was overruled.

155. I then persuaded Ms Chambers (over her equally strong objections) to appear in court because I considered her to be the most experienced and technically best in the area of counter code. I also chose Ms Chambers because I had complete confidence in her honesty and personal integrity to tell the court exactly what she was seeing in the Riposte message store, and I had confidence that she would not be rattled into saying anything other than what she was seeing in the message store.

156. I also informally de-briefed Ms Chambers after her evidence, and my recollection of the conversation was that she had found the experience very stressful.

GENERAL

Robustness

157. During my time working on Horizon, I was aware there were incidents that would affect the robustness of Horizon. Incidents that occurred during the overnight harvesting of transactions and subsequent processing of those

transactions, and separating them to different databases had the potential to have an adverse effect on POL and postmasters. I was also aware that there were incidents that related to apparent discrepancies in Post Office branch accounts, including in the Riposte software.

158. It was the function of the support teams to ensure that such incidents were handled correctly. Specifically in the case of the SSC, it was one of its functions to ensure that any workarounds were tested and implemented promptly, and to be involved in the process for resolving those incidents.

Postmasters' access to advice and assistance

159. Training of Post Office staff—both staff at Post Office branches and POL trainers—to use the system was entirely outside of my remit, as was the NBSC, which supplied assistance to any Post Office branch staff who were having difficulties, so I could not comment about any advice given to them on using the system.

160. I do not have direct knowledge of postmaster interactions with the NBSC, HSH, or SMC except where such conversations were relayed to the SSC in Peaks.

161. There was frequent interactions between the SSC technicians and postmasters, especially on Wednesday evenings after the introduction of Cash Account. If incidents had been passed from the SMC to the SSC relating to a counter issue, and if the exact nature of the issue was not clear, SSC technicians would phone Post Office branches and speak directly to the postmasters to understand their view of the symptoms, and would try to help them resolve the issue. Incidents regarding the Cash Account would originate from the NBSC.

162. It was necessary for the SSC to contact Post Office branches directly because no other part of the support hierarchy could view the Riposte message store. The ability to do so meant SSC technicians could match what the postmaster said they were doing over phone with the messages in Horizon.

163. Such interactions were controlled at the SSC end. The SSC would phone postmasters, but were encouraged not to give out SSC phone numbers to postmasters. This was to avoid the SSC being swamped by calls which could have been resolved by the NBSC and the HSH, and to ensure all calls were logged and auditable. The support lines were structured so that customers would start at 1st line support, and the call would be progressed up the lines of support based on the nature and severity of the reported issue.

Causes of problems experienced by postmasters

164. I think that, certainly in the initial phases of Horizon, there was a significant "culture shock" for POL staff and Post Office branch staff, moving from a manual, paper-based operation to a computer system. This was inevitable, for some of the postmasters this was the first time that they had used any sort of computer.

165. This "culture shock" was particularly true when Cash Accounts were introduced requiring the postmasters to balance their Cash Accounts every week. I recall that the SSC had to rota staff to work late, and on occasion development staff also, on Wednesday evenings, when the Cash Account was done to assist postmasters in completing the process.

166. I do not recall there being significant software bugs in EPOSS, but the Cash Account process involved a cross-reference between data from the counter and

manual counting of remaining stock and cash, if the two did not balance i.e., there was a discrepancy, then postmasters would call the helpdesks.

167. If the call was suspected to be a software issue, the SSC would check the message store contents and talk to postmasters to try to resolve the balancing issues/accounting differences in branch accounts.

Improving the advice and assistance to postmasters

168. I was not directly involved with the helpdesks which were the first point of contact—NBSC and HSH—and had no input or involvement in their processes. For these reasons, I do not have direct knowledge concerning the advice which they gave to postmasters.

169. In my opinion, and based on what I remember of the SSC workload and the comments from SSC staff at the time, in the early days of Horizon, I do not believe that there was sufficient correlation between, (a) the HSH scripts, (b) Post Office's procedures, and (c) what postmasters actually did. The result was that the helpdesks were unable to give advice to postmasters which was relevant to them. I also consider that the HSH, SMC and possibly NBSC were, initially, understaffed. Taken together, the impact was a higher than expected number of calls, and an unacceptable level of support.

170. In my opinion, the monitoring of Tivoli, and the configuration of that software caused problems for all support units. Tivoli "event storms" in which a huge number of events were generated had the potential to overload the staff monitoring Tivoli, and contributed to them missing other events. I remember SSC staff sometimes complaining that important events were missed because of event storms, but I cannot remember or provide further details.

171. Changes to the staffing levels and increased expertise in the helpdesks did improve the service provided. Over time, increasing familiarity and knowledge of the counter systems also enabled postmasters to resolve many of the issues they initially faced without helpdesk support. For example, I recall that the filtration rate improved from below 70% in 2000 to over 90% in 2006.

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated: 3. March 2023

INDEX TO THE FIRST WITNESS STATEMENT OF MR MICHAEL EDWARD PRYOR PEACH

Exhibit No.	URN	Document Description	Control No.
1	FUJ00079897	End to End Support Process Operational Level Agreement dated 17 June 2003	POINQ0086068F
2	FUJ00142216	Service Management Portal User Guide dated 22 December 2005	POINQ0148345F
3	FUJ00142217	Service Management Portal Support Guide 29 August 2007	POINQ0148346F
4	FUJ00142218	Service Management Portal High Level Design 19 July 2007	POINQ0148347F
5	FUJ00080096	Horizon Service Desk Joint Working Document dated 4 September 2008	POINQ0086267F
6	FUJ00080499	Call Enquiry Matrix and Incident Prioritisation – Software specification dated 23 April 2007	POINQ0086670F
7	POL00004074	Transcript Day 4 – March 14, 2019 – *Bates & Others v. Post Office Limited (No. 6) (Horizon Issues)*	VIS00005088
8	POL00004075	Transcript Day 3 – March 13, 2019 – *Bates & Others v. Post Office Limited (No. 6) (Horizon Issues)*	VIS00005089
9	POL00000678	Second Witness Statement of Richard Roll dated 13 March 2019, *Bates & Others v. Post Office Limited (No. 6) (Horizon Issues)*	VIS00001692
10	FUJ00079953	POA Customer Service Problem Management Process dated 29 July 2005	POINQ0086124F
11	FUJ00086334	Email from Lionel Higman to multiple recipients dated 18 July 2005 attaching "Note of Prayers" dated 18 July 2005	POINQ0092505F

Exhibit No.	URN	Document Description	Control No.
12	FUJ00086335	Note of Prayers dated 18 July 2005	POINQ0092506F
13	FUJ00086828	Peak PC0145617	POINQ0092999F
14	FUJ00120588	Peak PC0143500	POINQ0126780F
15	FUJ00084131	Insert Corrective Transactions at Branch 382137 dated 2 March 2009	POINQ0090302F
16	FUJ00088036	Secure Support System Outline Design dated 2 August 2002	POINQ0094207F
17	FUJ00084135	Host BRDB Transaction Correction Tool Low Level Design dated 13 November 2007	POINQ0090306F
18	FUJ00086866	Email from Mik Peach to Simon Ajina copying others dated 14 January 2009	POINQ0093037F
19	FUJ00087871	Email from Matthew Lenton to Jonathan Gribben copying others dated 25 June 2019	POINQ0094042F