Witness Name: Andrew Paul Dunks

Statement No.: WITN00300100

Dated: 20 February 2023

## POST OFFICE HORIZON IT INQUIRY

---

## FIRST WITNESS STATEMENT OF ANDREW PAUL DUNKS

---

I, Andrew Paul Dunks, will say as follows…

## INTRODUCTION

1. Since 2002, I have been employed by Fujitsu Services Limited in the Customer Service Post Office Account ("**CSPOA**") Security Team.

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 dated 4 January 2023.

## BACKGROUND

3. I have been asked to set out a brief professional background and the background to my involvement in the Horizon project.

4. I left school at the age of 16 and went to college to do an Engineering Industry Training Board (EITB) training course in electronics. I did not end up getting a job in that industry, but during training was introduced to my now wife, whose father had a business building residential extensions. I worked for him until he retired, and then worked for a company installing acoustic vents.

5.    In around 1996 a friend working for International Computers Ltd ("**ICL**") offered to get me a job in desktop computer support. I had no prior experience doing this sort of work. The job involved providing IT support internally to ICL employees. This was not connected to the Post Office and I was not providing external support to those outside ICL.

6.    ICL was acquired by the Fujitsu group and in 2002 changed its name to Fujitsu Services Limited ("**FSL**"). At that time, I was in the process of being made redundant. A vacancy became available in the CSPOA Security team within FSL, and in 2002 I was hired as the Cryptographic Key Manager for the team. I reported to the Operational Security Manager, who reported to the Chief Information Security Officer or 'CISO'. Throughout my time working on the Post Office account, I did not have anybody reporting to me.

7.    When I joined the Post Office account the Horizon project had already been rolled out. I was responsible for managing and refreshing the cryptographic keys that enabled the thousands of Post Office Horizon counter terminals to securely communicate with the Horizon system. Each cryptographic key had to be periodically refreshed. This involved using software to create new keys, and then pushing the keys out to the counter terminals. It was initially a very laborious manual process and took up most of my time. Following the roll out of Horizon HNG-X, the process of managing the cryptographic keys became much more automated and this was no longer such a significant part of my work.

8.    Over time, my role within CSPOA Security had expanded to include other areas of IT security such as user management, intrusion prevention and processing

applications for security checks. I was also given tasks not directly related to IT security, such as performing audit data extractions and transaction reconciliations. There were around five people in the CSPOA Security Team (though this number fluctuated over the years), and we would rotate through these different tasks on a regular basis, though some individuals had greater responsibility for certain tasks than others.

9.    User management involved maintaining a database of all the FSL employees with access to the Horizon system, setting the user permissions appropriate for their role, and managing the digital key devices (iKey) that they used to access the system.

10.   Intrusion prevention involved ensuring that anti-virus software was appropriately updated on the Horizon system.

11.   Processing applications for security checks involved providing administrative assistance to facilitate the vetting being carried out on new sub-postmasters ("**SPMs**"). For example, we would check the passport of the SPM and then send it to Group Security; if the security check came back as approved, we would then print off a pass for the SPM.

12.   Audit data extractions involved responding to audit record queries ("**ARQs**") made by the Post Office for archived data regarding transactions on the Horizon system. Each ARQ would specify the relevant post office branch, date range, and data type to be extracted. The person doing the extraction would logon to one of the dedicated secure audit workstations and enter the parameters specified in the ARQ into the audit extraction tool. The system

would extract the relevant data and export it to a spreadsheet. We would then place this spreadsheet onto a compact disc and send it to the Post Office.

13. Transaction reconciliation involved dealing with transactions that had got stuck, and had not completed. This was a very process driven task, and my role was to follow the documented procedure; I did not need to understand the technical details about how or why the transactions were getting stuck. However, in general terms I understood that there were many potential reasons that a transaction could get stuck, for example, because of a power or network outage. I understood that each transaction would go through a number of different 'states' until it reached the other end and cleared; if the transaction had not cleared then it would get stuck in a particular state, for example 'state 4' or 'state 23'.

14. There were three ways in which the CSPOA Security Team might be requested to assist with the transaction reconciliation process: (1) via automated reports; (2) by the Post Office finance team; and (3) by the Horizon System Helpdesk/Service Desk (the "**HSD**") or Software Support Centre ("**SSC**").

15. Reports would be generated each morning showing all the stuck transactions and which state they were in. This was the main way through which the team became involved in transaction reconciliation. Depending on the state the transaction was stuck in there would be a different procedure that we were required to follow. This would include reporting the stuck transactions to the Post Office through a Business Incident Management Service ("**BIMS**") report, and raising a PEAK (FSL's internal incident management system) for the SSC

to investigate. Once the SSC had resolved the issue, we would then update the BIMS report and send it to the Post Office.

16. I understood that these transaction reconciliation reports were automatically generated and did not rely upon, or arise from, errors reported by users. My role was to follow the procedure for raising a PEAK to the SSC to investigate the transaction, and to report the stuck transactions and the eventual resolution to the Post Office via BIMS.

17. On occasion, the Post Office finance team would contact us directly, or via the HSD, about a transaction reconciliation issue that had been raised to them, for example by an SPM. On those occasions my role would be to ensure that we had the necessary information about the transaction, to check whether we were already aware of it from the automated reports, and, if necessary, to raise a PEAK for the SSC to investigate. I would then report back to the Post Office finance team to confirm that the transaction was under investigation, and once the issue was resolved.

18. Finally, where SPMs contacted the HSD directly to raise a transaction reconciliation issue, then I understood that the HSD could refer this to the SSC for investigation. The SSC might then ask the CSPOA Security Team to check whether the transaction was already on the automated reports and under investigation. If the HSD contacted the team directly, then we would check whether the transaction was already under investigation, and, if necessary, raise the matter to the SSC.

19. I have been asked to describe my role in the investigation of errors reported by system users. I did not work on the HSD and did not communicate directly with

SPMs. Aside from my limited role in the transaction reconciliation process described in paragraphs 13 to 18 above (which was largely in response to automated reports and did not generally relate to errors reported by system users), I had no role in the investigation of errors reported by system users.

20. On occasion, I was requested to provide the Post Office with records of calls made to the HSD by a particular post office branch and (if requested) to summarise these in witness statements. While I therefore did have access to the historic HSD call records, I would only be looking at them when requested to do so as part of this task. I was not party to the calls themselves and had no role in investigating any errors (except as described above in relation to transaction reconciliation) or communicating with system users about them.

## ADVICE AND ASSISTANCE

21. I have been asked to explain how the HSD worked and my role within it, including the various reporting lines and how problems were escalated. I did not work within the HSD and had no role within it. While I know in general terms what the HSD did, I cannot say in detail how it worked, what the reporting lines were or how problems were escalated within it.

22. I am also asked to explain how calls were prioritised and whether this affected how problems were escalated. As I did not work within the HSD I cannot say how calls were prioritised by the HSD, or what effect this had on how problems were escalated.

23. I am aware that the HSD recorded calls on the TRIOLE for Services ("**TfS**") system, but that if the matter required further investigation it would be

transferred from the TfS system to the PEAK system. I am also aware from PEAKs that I have raised myself that incidents can be categorised as either A, B, C or D. Category A is the highest level of priority and I believe required a resolution within four hours. Category B required a resolution within eight hours and categories C and D had longer time limits.

24. My attention has been drawn to a Peak Incident Management System report for call reference PC0223333 raised on 4 February 2013 (**FUJ00082289**). This is an example of a PEAK raised by me as part of the transaction reconciliation process that I describe at paragraphs 13 to 18 above.

25. The PEAK summary states: "Branch 153113 – NB102 Section 5 EPAY – State 4 and Failed Recovery". From this I understand that this PEAK relates to an EPAY transaction at the stated branch which is stuck in 'state 4'. This transaction would have been on one of the transaction reconciliation reports generated for that day, and I would have been tasked with following the relevant procedure for a transaction stuck in state 4 by raising a PEAK for the SSC to investigate.

26. The summary also references 'Failed Recovery'. This is a reference to a separate report also generated each day. Quite often a stuck transaction would be resolved automatically when the SPM rebooted their counter terminal the following day. If not, then I understood that the transaction would additionally be listed on the failed recovery report. The transaction being discussed in FUJ00082289 is listed in both reports, and I am making the SSC aware of this in accordance with the procedure.

27. Aside from changing the relevant transaction details, the majority of the text in my initial entry at 09:13:33 will have been copied and pasted from our standard procedure for dealing with a transaction stuck in state 4.

28. I have been asked what I meant by the words "*PLEASE include further txn attempts with the same PAN immediately after this txn if applicable as this is useful for Post Office Ltd for settlement issues.*" My recollection is that these words formed part of the standard procedure for dealing with a transaction stuck in state 4 and I copied and pasted them into the PEAK.

29. I was not the original author of these words, but I understand them to be an instruction to the SSC to look at other transaction ('txn') attempts with the same Primary Account Number or 'PAN' (the unique reference number associated with the payment card) immediately following the stuck transaction. I understand that such information would be useful for the SSC's investigation in order to ensure that the transaction was settled correctly (i.e. that the funds were correctly debited and credited to the relevant accounts). For example, this would show if multiple payment attempts had been made with the same payment card.

30. My attention has also been drawn to an entry from the Known Errors Log ("**KEL**") database with reference number acha1717T titled 'Branch reports an unexplained discrepancy' raised by Anne Chambers on 30 July 2010 (**FUJ00082302**). I understood that the KEL was maintained and used by the SSC for the purpose of investigating and recording errors. While I, in common with many others, had access to the KEL, I would not routinely view KEL

records and had no responsibility for writing them. My name is not referenced in this document, and I have no recollection of ever having seen it before.

31.  Aside from my involvement in the transaction reconciliation process, described in paragraphs 13 to 18 above, I was not responsible for dealing with discrepancies raised by end users and have no knowledge about what Fujitsu's policy was in relation to unexplained discrepancies.

32.  I am asked to consider the following extract from FUJ00082302: "*When responding, if they have given specific examples that you can explain, do so; otherwise make clear it is not a system problem (assuming you have checked that everything adds up). See PCPC0229446 for an example response which may help with the wording.*"

33.  I have not been provided by the Inquiry with a copy of the document being referred to in this extract and have no recollection as to whether I have ever seen it, or what it contains. I am not the author of FUJ00082302 and cannot comment on the purpose of the example response.

34.  I am asked to describe the process by which the HSD operators were expected to 'check that everything adds up', and whether there was a mechanism within Fujitsu for HSD operators to escalate with the Post Office or Fujitsu any particular trends or issues that emerged. As I was not an HSD operator, I cannot comment on these questions.

## KNOWLEDGE OF BUGS AND ERRORS

35.  I am asked how trends in issues notified to the HSD operators by SPMs were monitored and recorded. In general terms, I understood that SPMs would

contact the HSD and that HSD operators would make records of the calls on the TfS system. I understood that where issues required further investigation the call would be transferred to the PEAK system and referred to the appropriate team, such as the SSC. I also understood that known errors could be recorded by the SSC in the KEL. However, as I did not work within the HSD or the SSC I am unable to provide any details about how any trends in such issues were monitored or recorded.

36. To the best of my recollection, aside from the transaction reconciliation process described in paragraphs 13 to 18 above, the only other occasion on which I had any involvement with the calls being raised by SPMs was when I was asked to provide extracts of the archived HSD call records to the Post Office. While I was sometimes asked to summarise in a witness statement the nature of the issues being raised in those records by a particular branch, I was not responsible for performing any analysis of trends in issues being raised by SPMs more generally.

37. I am asked to consider a document titled 'Reconciliation and Incident Management Joint Working Document', dated 18 March 2013 and authored by 'Donna Munro, CS Security, Fujitsu Services' (**FUJ00085359**). Ms Munro was the Operational Security Manager, and my line manager, at the time.

38. I am named in the distribution list for the document, along with others. I note that that the document was issued to me 'for information' only and that I was not on the list of mandatory or optional reviewers (pages 4-5). I was aware of the existence of this document, and would likely have referred to it from time to time as necessary, but had no involvement in its creation or review. As I have

said, my role was very process driven and I did not need to understand how or why everything worked; I simply needed to know which process to follow in a particular situation.

39. I am asked to describe how reconciliation errors were reported and by whom, what happened when an error was notified and how it was investigated, and what action was taken in response to the notification of such errors and by whom. I have described the process of dealing with transaction reconciliations in paragraphs 13 to 18 above.

40. I am asked to consider an excel document last modified by Matthew Lenton on 10 January 2019 at 5:23pm which appears to be a list of tasks created between 2006 to 2018 (**FUJ00087700**). I have no recollection of ever having seen this document before. It appears to be a list of tasks associated with particular change requests. I note that the document lists 19,435 lines but has been filtered to show just 61 tasks, none of which were last updated by me. A total of 331 tasks within this document were last updated by me. I note that many of these 331 tasks relate to failed recovery or delayed transactions, which was part of the transaction reconciliation process that I describe in paragraphs 13 to 18 above. Many of the other tasks last updated by me relate to OBC19 requests; these were requests from the Post Office for updates or changes within the Post Office Data Gateway (PODG), the automated file transfer system used for transferring files between the Post Office and third parties such as financial institutions and utility providers.

41. I am asked to describe the method by which errors were escalated by Fujitsu, the process for logging errors and who had access to historic error logs.

42. In respect of the escalation and logging of errors, in general terms I was aware that there were various lines of support through which issues/errors could be escalated. The HSD provided 'first line' support to end users experiencing issues with Horizon. TfS call records would be kept by the HSD of the issues raised. Where an issue raised required further investigation, the TfS call would have been transferred to the PEAK system, for action by the appropriate team, such as the SSC. I understood that where the investigation concluded that a change was required to the Horizon code, that this would then be escalated to the software developers to make the change, test it, and then roll it out. As described above, I also understood that the SSC could record known errors (and, if applicable, how to resolve them) within the KEL database. However, I was not involved in that process.

43. In respect of access to 'historic error logs' (which I understand to mean the KEL), my understanding was that anyone who had access to the PEAK system would have been able to access the KEL records. I was able to click into or search for KEL records through the PEAK system, and did view some such records on the occasions that this was required for my role. The PEAK system was widely used within CSPOA for assigning actions on tickets to particular teams, so many people needed to have access to the system. As far as I was aware, once a person had been given access to the PEAK system they had full access to all records held within it, and could therefore have accessed any of the KEL records.

44. My attention is drawn to a KEL record titled 'Multiple cash declarations may cause incorrect figures in Discrepancy, Variance and Balance Reports' raised

by Mark Scardifield on 15 July 2005 with reference number MScardifield2219S (**FUJ00082274**). I am not named in this document and I have no recollection of whether I have seen it before.

45. I note that the KEL record was last modified by Anne Chambers on 27 November 2007 and the type is shown as 'unresolved'. I am asked whether there was a process in place to deal with issues marked as unresolved. I did not work within the SSC and was not responsible for investigating such issues, creating or maintaining the KEL, or tracking whether issues recorded in the KEL had been resolved.

46. I am asked to look at a spreadsheet last modified by Pat Lywood on 17 June 2010 at 10:55am, which according to the 'Preamble' worksheet appears to have been prepared for the 'CS Prayers' meeting (**FUJ00084433**). I am aware that the CS (Customer Service) Prayers meeting took place every morning and was attended by CSPOA management. As far as I can recall, I have never attended a CS Prayers meeting, and as far as I am aware, I have never seen this document before. The document appears to list various PEAKs and to track the progress of their investigation and resolution, however, as I was not present at the CS Prayers meetings, I cannot say how it was used.

47. My attention is drawn to item 622 on the 'Detail' worksheet which relates to PEAK PC0198077, described as "*This is where following rollover, if there is a discrepancy, the branch is able to clear their local suspense multiple times.*" I note that my name is not mentioned anywhere in connection with this item. As far I am aware, I had no involvement in dealing with this issue; this is not the sort of thing that I would be dealing with as part of my role.

48. I have been asked to describe the function of the 'local suspense' account and whether the issue described in item 622 was rectified. I do not know what a local suspense account is, and do not understand what it is that item 622 is describing. I have no knowledge as to whether the issue was rectified. As such, I cannot say how it was rectified, what steps were taken in relation to it by anyone, or whether Fujitsu informed the Post Office or the relevant SPM about it.

## INTEGRITY OF THE SYSTEM

49. I have been shown copies of various internal security audit/assessment reports. I am asked to explain why internal assessments or audits of the system were carried out, the process by which they were carried out by Fujitsu, how the results of previous assessments or audits were traced and what records were kept of them.

50. I was not responsible for carrying out or managing internal audits or assessments, though I was on occasion asked questions as part of the audits that were carried out.

51. In general terms, I understood that the purpose of carrying out an internal assessment or audit was to ensure that our internal documented processes were in compliance with the applicable national and international standards, and that we were operating in compliance with our own documented processes.

52. I also knew that CSPOA would be externally audited against these standards. One of the purposes of the internal audit was therefore to ensure that we were

in compliance with the standards, and that any non-conformances were addressed, prior to the external audit taking place.

53. I was not involved in conducting the audits, so cannot say how exactly they were carried out, save that I was aware that the auditors would look at documents and raise questions with relevant personnel. For example, I can see from a document titled 'Local Security Audit Report - Networks – 2009', dated 18 August 2009 and authored by Nigel Hatcher, RMGA Quality Manager (**FUJ00080805**), that I was contacted by the auditors by email regarding the appropriate classification of a document that I had written about the process for out of hours support team members who needed to change their passwords. It appears from the report that I responded by email to explain that as the authentication process for access to the system had changed, the document that I had authored was now obsolete and would not be taken forward. This type of exchange typified my involvement in the audit process.

54. Following the audits, I understood that a report would be produced by the auditors which would record any non-conformances, observations and required corrective actions. Where corrective actions were assigned to me, I would complete them. I assume that the auditors had some way of tracing the actions raised and whether they had been completed, but I was not responsible for this process and so cannot comment on how it worked.

55. I am aware that reports were written following the audits/assessments, as some of these were sent to me. However, I do not know what other records were kept by the auditors of the work they carried out.

56.    I am asked to consider a spreadsheet last modified by Pat Lywood on 8 June 2010 at 10:38am, which appears to be a version of the CS Prayers spreadsheet described above, but from a different date (**FUJ00084385**). Again, I did not attend these meetings and have no recollection of having seen this document (or any other version of it) before.

57.    My attention is drawn to item 192 on the 'closed' worksheet of the document which relates to PEAK PC194590, described as "*Duplicate JSNs present in the HNG-X counter audit trail*". I note that, as with item 622 addressed above, my name is not mentioned anywhere in connection with this item.

58.    I am asked to explain the following comment recorded in the document in respect of this item: "*From an Audit perspective this is a bit of a disaster. The Audit system uses the JSNs to confirm the completeness & integrity of retrieved audit data. This retrieved data may well end up being used in court cases to support POL prosecutions for fraud etc. The presence of duplicates or gaps in the JSN sequence would totally discredit this data and would probably end up supporting the usual defence claim in such cases that any financial losses were as a result of errors within the system*".

59.    I understand that each transaction that took place on each Horizon counter terminal was assigned a Journal Sequence Number ("**JSN**"), and that each sequential transaction on the terminal should be assigned a sequential JSN.

60.    I recall that an issue arose in around 2010 with the data that we were exporting in response to ARQs made by the Post Office. I recall the issue involved there being both gaps in the data that we were exporting (i.e. the JSNs shown were not sequential) and duplicated transactions (i.e. transactions showing the same

JSN). My recollection is that we stopped doing ARQ exports for a short time while this issue was resolved.

61. While it is clearly a problem for there to be gaps or duplicates in any data, I am unable to comment on the impact that this might have on court cases, as this is outside of my expertise. The quoted extract was not my remark and so I cannot comment on why the author has said it.

**Statement of Truth**

I believe the content of this statement to be true.

Signed: GRO

Dated: 20/02/2023.

## Index to First Witness Statement of Andrew Paul Dunks

| No. | URN | Document Description | Control number |
|---|---|---|---|
| 1 | FUJ00082289 | Peak Incident Management System report for call reference PC0223333 raised on 4 February 2013. | POINQ0088460F |
| 2 | FUJ00082302 | Entry from the KEL database with reference number acha1717T titled 'Branch reports an unexplained discrepancy' raised by Anne Chambers on 30 July 2010. | POINQ0088473F |
| 3 | FUJ00085359 | Document titled 'Reconciliation and Incident Management Joint Working Document', dated 18 March 2013 and authored by 'Donna Munro, CS Security, Fujitsu Services'. | POINQ0091530F |
| 4 | FUJ00087700 | Excel document last modified by Matthew Lenton on 10 January 2019 at 5:23pm which appears to be a list of tasks created between 2006 to 2018. | POINQ0093871F |
| 5 | FUJ00082274 | KEL record titled 'Multiple cash declarations may cause incorrect figures in Discrepancy, Variance and Balance Reports' raised by Mark Scardifield on 15 July 2005 with reference number MScardifield2219S. | POINQ0088445F |
| 6 | FUJ00084433 | Spreadsheet last modified by Pat Lywood on 17 June 2010 at 10:55am, which according to the 'Preamble' worksheet appears to have been prepared for the 'CS Prayers' meeting. | POINQ0090604F |
| 7 | FUJ00080805 | Document titled 'Local Security Audit Report - Networks – 2009', dated 18 August 2009 and authored by Nigel Hatcher, RMGA Quality Manager | POINQ0086976F |
| 8 | FUJ00084385 | Spreadsheet last modified by Pat Lywood on 8 June 2010 at 10:38am, which according to the 'Preamble' worksheet appears to have been prepared for the 'CS Prayers' meeting. | POINQ0090556F |