Witness Name: Alan George D'Alvarez

Statement No.: WITN0480_01

Exhibits: WITN480_01/1 – WITN480_01/13

Dated: 9 August 2022

POST OFFICE HORIZON IT INQUIRY

FIRST WITNESS STATEMENT OF *ALAN GEORGE D'ALVAREZ*

I, *MR ALAN GEORGE D'ALVAREZ,* will say as follows:

INTRODUCTION

1. I am currently a Programme Executive at Fujitsu Services Limited ("**Fujitsu**") working in the Europe region, a position that I have held since April 2018. I am not currently involved with the Horizon IT system or Fujitsu's Post Office Account.
2. This witness statement is made on behalf of Fujitsu to assist the Post Office Horizon IT Inquiry with the matters set out in the Rule 9 Request provided to Fujitsu on 11 March 2022 and a series of follow-up questions provided to me by the Inquiry on 1 July 2022 (the "**Request**"), to the extent that I have direct knowledge of such matters.
3. The topics set out in the Inquiry's Request that I am able to comment on relate to matters that occurred up to 25 years ago. These relate to my involvement in the design and development of an automated key management system for Legacy Horizon in the period prior to the national rollout, and my involvement in the replanning, pilots and rollout of the Horizon Online system from 2008 to 2010. I have

tried to remember relevant events to the best of my ability. However, there are areas where my recollection is unclear or limited.

4. Where I have seen documents relevant to the Inquiry's Request for the purpose of preparing this statement or where I have referred to documents, these documents are referred to using references WITN480_01/1 – WITN480_01/13 and are listed in the index accompanying this statement. To the extent that these documents have not already been provided to the Inquiry, they are exhibited to this statement.

BACKGROUND

5. I joined ICL Pathway Limited ("**ICL Pathway**") in March 1997 to lead the delivery of security related elements of the Horizon IT system. At the time, I had previous experience of secure systems from my work with the Metropolitan Police. I continued in this role until December 2000.

6. I subsequently had a number of other roles on the Horizon project:

   a. January 2001 to August 2002: Applications Delivery Manager, Post Office Account: Responsible for creating and running a combined applications and infrastructure delivery capability from the previous five delivery units operating across the account. The capability was responsible for all application and managed infrastructure changes applied to the Horizon system to support the transformation of Post Office Limited ("**Post Office**") from a supplier of postal and government services to a high street presence extending into financial, travel and other retail services.

   b. September 2002 to June 2005: Director of Delivery, Post Office Account: Responsible for setting up and running the combined Unit responsible for design, development, integration, testing and deployment of new solutions. The Unit met the challenges of the new IT Roadmap initiatives whilst delivering to the Post Office change programme.

c. May 2009 to December 2010: Programme Director Horizon Online, Royal Mail Account: Due to significant delays, I was assigned to take responsibility for delivering Horizon Online. I led the re-planning and successful delivery of the programme.

JOINING ICL PATHWAY AND THE HORIZON PROJECT

7. When I joined the Horizon programme in March 1997, the programme was working on various "releases" of the Horizon system. At the time, there was Release 1A, 1B, 1C and then Release 2. The pilot of Release 1A had already been completed by March 1997 and, as I had no involvement in it, I cannot comment on the date that it started. I understand this pilot to be what the Inquiry refers to as the "Initial Go Live" pilot. At the time I joined, Release 1B was in the final preparation for deployment to a limited number of Post Office branches – about 200. Release 1B occurred around approximately June 1997. Release 1C followed in early 1998 and I believe the pilot was then extended to a further 100 post offices. I understand these two pilots to be what the Inquiry has referred to as the "*further software releases at approximately 200 – 300 post office branches between 1997 – 1998*". I do not understand the Inquiry's references to a "*full live trial*" of the Horizon IT system. However, I was involved in the Horizon project during the pilot of New Release 2, which commenced in late 1999, and which involved a larger number of Post Office branches than the

previous pilots (Release 2 having been renamed following the Benefits Agency's withdrawal from the project). I address that involvement below.

8. From the time I joined ICL Pathway, up to and including the release of New Release 2, I was involved only in the security aspects of the Horizon system, and any aspects of this statement relating to that period are given on that basis. The team working with me on these security aspects numbered up to 50 people, but included Roy Birkinshaw (Security Development Team Lead), Dave Johns (Security Architect), Belinda Fairthorne (Security Consultant) and Tom Parker (Technical Security Consultant).

IDENTIFYING DEFICIENCIES IN THE SECURITY OF THE HORIZON IT SYSTEM

9. When I joined the Horizon IT project in March 1997, I assessed the system security requirements that ICL Pathway had contracted to deliver and the solution it had proposed to meet those requirements. I identified a number of areas where we needed additional or different solutions to ensure compliance with the contractual requirements. These were an automated key management system ("**KMS**") and processes to address requirements for access controls in relation to privileged users as a result of the completion of the Access Control Policy

10. A key feature of the security system, when I joined the project, was that in order for a postmaster to access the Horizon system on their Post Office branch counter, they would need to have a password and a physical cryptographic memory card (a "**key card**"). This solution was to address the requirement for two-factor authentication at the Post Office counter.

11. This was to address Post Office security concerns around unauthorised people being able to access the Horizon counter. Specifically, a password-only system was not thought to be enough and system access requiring a physical device and a password was implemented. This decision and the discussions that led to it occurred before I joined the Horizon programme, and so I was not party to them.

12. While I was not involved in the pilot of Release 1A, my understanding from my later work was that, in that pilot, there was no key card entry system at the Horizon counters. Given my lack of involvement in the Release 1A pilot, I cannot comment as to why a key card entry system was not present in Release 1A. However, by the Release 1B pilot, such a system had been added.

13. Prior to the Release 1B pilot, it was identified that the recovery process in place for the pilot was not a supportable solution or operationally fit for purpose at scale. By the "recovery process", I mean the process by which a key card would be replaced if it was lost by a postmaster.

14. The recovery process during the Release 1B pilot was a manual Diffie-Hellman exchange done over the phone between the postmaster and the Horizon support desk. A Diffie-Hellman exchange is a secure means of cryptographic recovery.

15. If a postmaster lost their key card, they would phone the Horizon support desk. In order to go through the recovery process, the postmaster had to click through 15 screens of lengthy random alphanumeric numbers on their Horizon counter, and provide those numbers to a member of the Horizon support team within a secure location at the Horizon support desk. The support desk would, in turn, also click through 15 screens of lengthy random alphanumeric numbers and they would provide

those to the postmasters for entry on their counter. This process verified the authenticity of the counter and the postmaster's identity and enabled a secure key, unique to that post office, to be downloaded onto a spare blank key card held at the post office. At the end of the process, the blank key card would be loaded with a new secure key and the post master would be able to access the system.

16. This was a really cumbersome and time-consuming process. A Post Office branch could not trade until this process was completed as the postmaster would not have access to their counter. The postmaster and service desk also had to do the exchange over the phone, so there were often miscommunications. This process took, at best, 15 minutes to complete.

17. This manual approach to key card recovery was demonstrated by the Horizon security team to Jeremy Fawkes (Head of IT Security at the Post Office) and Gareth Lewis (Director of Security, Benefits Agency) in March 1997. At a meeting that followed the demonstration, Jeremy raised that the manual approach was not a supportable solution or operationally fit for purpose at scale, and placed an action on the Horizon security team to look for a more sustainable solution.

18. My understanding, which I think may have come from conversations with Jeremy Fawkes, was that the Post Office was concerned about the business impact of a postmaster losing their key card and the time it would take to recover the key card to enable the post office to trade. My understanding at the time was that if the system was not available to a postmaster, the Post Office would have had to pay compensation to the affected postmasters for loss of trade, and this was a big concern for them. In addition, ICL Pathway had the challenge of refreshing keys held on the

key card periodically to conform to the Communications-Electronic Security Group ("**CESG**") guidelines which the manual recovery process would not be able to support.

19. My understanding is that whilst the Joint Authority (Post Office and Benefits Agency) had signed off on the pilot of Release 1B, they would not sign off general deployment of the system until a more acceptable key card recovery solution was in place. I believe that decision was taken around the time the roll-out of Release 1B was approved, though my recollection is not certain.

OBTAINING APPROVAL FOR A KEY MANAGEMENT SYSTEM

20. I was actioned to provide a more sustainable and supportable solution for key card recovery, which after analysis of the operational and support requirements led to the proposal of implementing an automated secure key management system ("**KMS**").

21. The contract for the Horizon system between ICL Pathway, the Post Office and the Benefits Agency (the "**Horizon Contract**"), and the business needs reflected in the Horizon Contract, were the main drivers for any design and development on the project, coupled with the supportability of any proposed solution. My understanding of the Horizon Contract was that ICL Pathway had signed up to deliver a secure system. The system we had in place during Release 1B was secure, but the recovery process for a lost key card was complex and not sustainable for a large number of post offices, nor would it support an estate wide key refresh.

22. Of course, I understood that the Horizon IT Contract did not say that we specifically needed to deliver a KMS (and as I was not involved in the negotiations of the Horizon Contract, I cannot comment on why the matter was not considered as part of the original negotiations). However, after an assessment of the options, it was concluded

by the security team that an automated KMS was the appropriate way forward for reasons of usability and to avoid the impacts to the Post Office business of not having one in place (as more particularly explained at paragraphs 16 to 18 above).

23. A big challenge was that we contracted to use the “Red Pike” cryptographic algorithm sourced from the CESG and that a KMS would need to conform to the mandated polices and controls applicable to cryptographic algorithms supplied by CESG.

24. The KMS proposal, prepared by myself, Roy Birkenshaw and Dave Johns, was presented to the ICL Pathway Board that consisted of John Bennet (CEO), Tony Oppenheim (Finance Director), John Dicks (Requirements Director), Martyn Bennett (Director, Security and Risk Management), Liam Foley (Business Development Director), Terry Austin (Director of Delivery) and Steve Muchow (Service Director). This presentation occurred around July or August 1997, and I believe the proposal was documented in a document titled ‘the KMS Solution Overview’. I recall resistance to the proposal and a debate with Tony Oppenheim, who questioned why ICL Pathway needed to absorb the cost of additional security. This would be a significant investment for ICL Pathway as the costs of developing the KMS would not be recoverable from the Post Office/Benefits Agency under the charging mechanisms in the Horizon Contract. In particular, his view was that the Post Office and Benefits Agency had signed up to a Microsoft Windows NT based solution, which included the limitations of that technology. Microsoft NT is a computer operating system which supports a computer’s basic functions. Part of such systems contain an element of security controls to protect a device, data stored and the transfer of data. However, Windows NT did not support the specific requirements associated with the

management of CESG supplied algorithms. During the presentation, the proposal was approved given the need for it and the overall benefit it would bring to both service and the customer.

DESIGN, DEVELOPMENT, TESTING AND ACCEPTANCE OF THE KMS

Design

25. At the time, the processes for design and development of new software at ICL Pathway followed a standard approach. It was a typical waterfall methodology that was standard for IT projects at the time. The steps were business analysis, design, build, integration and then test. My recollection is that the following individuals led teams that were responsible for this process on the Horizon project prior to the national rollout of the Horizon system:

    a. Dick Long: Design

    b. Chris Humphreys: Development

    c. Chris Wannell: Integration

26. In relation to the design and development process for the KMS, I believe that there would have been templates for designs and testing. There was a defined set of processes at each stage of the methodology and there should be templates showing that. I recall dealing with an ICL capability, headed up by Jules Oliver, called "Application Management" who assigned a team to work on the design and build of the KMS. This team was led by Roy Birkinshaw who reported into me. I was the approval authority for the delivery plans and key requirement documents.

27. Further information about the design of the KMS may be found in the Key Management High Level Design Document dated 10 March 1999 (WITN480_01/1).

Testing

28. The KMS then went through testing and user acceptance. While I have a general awareness of ICL Pathway's testing procedures as a member of the Horizon Programme, I was not responsible for testing. I cannot remember who was responsible for testing at the time.

29. Based on my general understanding, at the time, ICL Pathway had the following test phases:

    a. System Test

    b. Security Test

    c. System Integration Test

    d. Performance and Integrity Test

    e. Release Test

30. Within ICL Pathway, we made use of agencies and partner organisations to resource test teams, but any testing carried out by ICL Pathway was managed internally. The customer was responsible for the User Acceptance Test ("**UAT**") and supplied their own team for this.

31. I have had an opportunity to consider WITN480_01/6, which are minutes of a meeting I attended between ICL Pathway and Utimaco on 5 November 1998. Utimaco were the suppliers of the Virtual Private Network ("**VPN**") hardware devices that were chosen for Horizon. A VPN establishes an encrypted link to securely transmit data and, in Horizon, was used to encrypt data between the data centres, Post Office branches and other third party interfaces. My recollection is that the design for Horizon's VPN was completed by Alex Robinson supported by Utimaco, who supplied

the encryption devices. Utimaco would provide support to the Fujitsu test teams validating this element of the solution. As such, if a PinICL was raised that was due to a fault in the supplied VPN encryption devices, a support ticket would be raised against Utimaco to investigate the issue and, where required, Utimaco would deliver a fix.

32. The KMS went through the Security Test, System Integration Test, Release Test and UAT. The Security Test Team reported to me. Defects raised against security products, including the KMS, were triaged by myself, Dave Johns and Roy Birkinshaw prior to being allocated to teams for resolution. The defect management process generally operated as follows:

    a. A PinICL would be raised by the test team to record a system fault that is causing a test failure within a test script.

    b. Defects would be triaged to (i) confirm that the test failure is as a result of a fault in the solution (as a test failure may not be a system fault, for instance because the test script was incorrect or an incorrect procedure followed, (ii) determine which resolver group (team) to allocate the defect to for resolution and (iii) propose defect impact and priority.

    c. The Post Office and Benefits Agency, as Joint Authority, would confirm the business impact of the defect.

    d. Fixes would be delivered by the resolver group and the test would be re-run, or the fix inspected (in the case of amendments to documentation).

    e. At the conclusion of each test phase, a test report would be completed which identified any defects that were unresolved at the point of exiting that test phase. It is possible that a defect open at the end of one test phase may be resolved in a future test phase and prior to the completion of all test phases.

f. At the point acceptance was reviewed, any unresolved defects would be included in an acceptance report. From recollection, a system could not go live with any open defects that were considered "high priority" by the Joint Authority, and any "medium priority" would need to be supported by a work round procedure where applicable. The Joint Authority would take into account the open defects as part of their decision to go live with the solution.

33. Whilst I do not recollect specific defects I have reviewed a copy of a PinICL, PC0005088, related to the KMS (WITN480_01/7). I would say that this is typical of a fault found in testing, where a security issue was highlighted in respect of system access. As can be seen in the PinICL record, changes were made to remove this access mode and an alternative secure access route and procedure was introduced. The PinICL also confirms that the proposed resolution was approved by Jeremy Fawkes. Defects would generally fall within the following categories: Technical (requiring a system change to resolve), Process (requiring a change of approach/procedure to resolve), Documentation (requiring an amendment to documentation). The above PinICL PC0005088 is an example of a Process issue.

Acceptance

34. Following testing, the final KMS solution was then signed off through acceptance. Generally, it was the programme managers who dealt with acceptance at the time. I am not sure, but I recall that the programme manager who took us through the pilots

was Martyn Hughes. Martyn reported to Terry Austin who oversaw software development, test and deployment. He would oversee all software development up to acceptance into service.

35. I am not aware of any changes to the acceptance criteria for the security of the Horizon system during the period I was involved in the development of the KMS or at any other time.

Delays

36. The Post Office and Benefits Agency allowed the pilot of Release 1C to go ahead without the KMS being deployed, though I have no knowledge as to why that decision was made. However, the KMS was required for the larger scale pilot of New Release 2.

37. From my perspective, the security and development of the KMS contributed to the delay of the New Release 2 pilot and the subsequent roll out of Horizon for two major reasons:

    a. We had to implement the security requirements from the Access Control Policy (WITN480_01/2) and the Security Functional Specification Document (WITN480_01/3), which described the technical security specifications for the Horizon system. I note that I reviewed the Pathway Security Policy dated 8 October 1996 (WITN480_01/4) in order to assist with my recollection of the two documents just mentioned. Many of these requirements were not previously implemented in Releases 1A, 1B, and 1C, but they were required for New Release 2. In fact, I believe the Access Control Policy had not even been signed off when I joined in March 1997 and when the earlier pilots were under way. Developing the technical control procedures to meet these two documents took time.

b. My team also needed to clear defects raised through testing and resolve them prior to the go live of New Release 2. Not all defects that we had agreed with the Post Office should be fixed before going live had, in fact, been fixed in the planned timescales. I think I needed another two months from my original test plan to get through my defect clearance. I am not aware of whether sub-postmasters were informed of these defects, and it would not have been part of my role or responsibilities to interface with sub-postmasters. The Post Office had in place two people who were accountable for overseeing security testing. I cannot remember their names, though the first name of one of them may have been Cliff. They were accountable for reviewing all defects and agreeing the business priority of those defects. They also reviewed the position around unresolved defects at the point of exiting the security test phase, and they audited test results and PinICL content for accuracy. I was not sighted on any of the reporting these Post Office representatives may have done (including to whom they reported) within the wider Post Office organisation.

38. Having reviewed a copy of the Exception Plan for Delivering KMS (WITN480_01/8), I am reminded that a decision was made to split the delivery of the KMS into two phases in order to meet the New Release 2 deadline. As the Exception Plan highlights, the sheer volume of work resulted in the development team falling behind schedule. Three options were considered and the option agreed was to phase the delivery of the KMS.

The first phase was to deliver all solution components required to support key refresh associated with lost/not working Post Master Memory Cards (PMCCs). The second phase, to be delivered post go live of New Release 2, was to deliver the additional functionality required to enable a global key change across the whole estate to take place. Global encryption key changes would be undertaken every 12 months and therefore the second delivery phase would need to be implemented within 12 months of New Release 2 going live. I recall that this second phase was delivered within the 12 month period. The document titled 'Requirements for KMS at CSR+', which is referred to in the Exception Plan, is also exhibited to my statement at WITN480_01/9.

39. Besides the matters described above at paragraphs 37 and 38 above, I do not recall any other matters under my supervision which caused delays to Release 1C or New Release 2. My recollection is that no changes were made to the original specification.

40. However, the implementation of security was not alone in causing the delay to the New Release 2 pilot. While I do not recall the details, there were a number of other delays across the project in the run up to the New Release 2 pilot.

THE NEW RELEASE 2 PILOT

41. I do not recall the specific nature of problems or issues that were raised during the New Release 2 pilot.

42. Generally, I understand that during the New Release 2 pilot, incidents were raised through the service desk for any issues encountered. Where the resolution required a code fix, this would be passed to 4th line support where a defect would also be raised and tagged to the incident. The defect would be annotated with the cause of the defect and the resolution. I suggest that the incident system may be searched for

any ticket raised by a pilot site that has a corresponding defect number to identify technical issues raised during the pilot phase.

FITNESS FOR PURPOSE OF THE HORIZON SYSTEM PRIOR TO ROLLOUT

43. Before the national rollout of the Horizon system, a penetration test was conducted by an independent third party appointed by the Post Office in order to validate the security of the Horizon IT system. I do not independently recall the name of the organisation that conducted the penetration test, but I have reviewed ICL Pathway Change Proposal No. 1987 (WITN480_01/10), which indicates it was Admiral Management Services Limited.

44. A penetration test is a test to assess the security controls implemented in the production or "live" environment. A report was prepared by the tester with critical, high, medium and low issues. I believe it was sent to Barry Proctor, who was the Chief Information Security Officer at ICL Pathway and the originator/sponsor of ICL Pathway Change Proposal No. 1987. My security team then reviewed that report with the Post Office and agreed with them which issues needed to be fixed. We raised defects for any issues that we had agreed needed to be fixed.

45. I also recall that a team from Fujitsu Japan came to ICL Pathway to conduct an audit of the Horizon project around the time the business was negotiating the new contract with Post Office after the Benefits Agency had pulled out. I think, but I am not sure, that it was mainly a design audit and Dick Long and Dave Johns were directly involved. I recall being asked questions about the KMS as part of that audit. I have no other recollections of the audit. I do not remember receiving its outcomes or to whom they might have been addressed.

46. I did not have any concerns in respect of the fitness for purpose of Horizon.

HORIZON ONLINE

47. In 2008, I was not working on the Horizon project but was working on the bid for the Passport Enrollment as part of the National Identity Scheme.

48. At that time, I was asked by Lester Young and Pete Jeram to conduct a review of the Horizon Online project. I understood that the Horizon Online project was failing to deliver, encountering constant delays and that the Post Office was losing confidence in the project. From my review, I concluded that the project was driven to achieve dates rather than quality. Evidence of this was that test phases were reported as having started when a number of the solution components required to make the testing valid had not been completed. There were also many cases of development being reported as complete when the supporting design was still incomplete or in draft status. I recall that a number of the individuals interviewed as part of the review openly stated that the focus was on getting milestone sign off without due consideration of the completeness of the deliverables associated with that milestone.

49. I do not recall them in detail, but I made several recommendations in a report following my review. In preparing this statement, I have not seen a copy of the report and am unable to recall identifying details about it.

50. I then worked on a replan of the project based on my recommendations for the remainder of 2008. The replanning involved: (i) a review of Horizon Online's scope and associated deliverables, and confirmation that these met the requirements of the contract, (ii) a review of progress at the time against deliverables, (iii) a review of estimates as to time and resources for remaining deliverables, based on actual

figures from completed deliverables, (iv) the scheduling of remaining activities to complete outstanding deliverables, (v) a review of the schedule and an assessment of schedule contingency, (vi) a review of overall resource requirements and forecast costs, and (vii) a review and update of the programme Risk, Issues, Assumptions and Dependencies log against a revised schedule for completion.

51. The replan involved a range of individuals over five stages:

   a. Stage 1: This involved all Fujitsu Horizon Online work stream leads, supported by their team leads. These were David Johns (HNG-X Chief Architect), Roger Goldsmith (Application Development Lead), Vince Cochrane (Infrastructure Lead), Debbie Richardson (Test and Validation Lead), and Lee Farnham (Post Office Test Assurance Lead). I also recall involvement of the Integration Lead and the Deployment Lead, but do not remember their names.

   b. Stage 2: This was an independent validation of the replan by the Fujitsu Delivery Assurance team

   c. Stage 3: These were joint sessions with the Post Office programme management team (led by Mark Burley). The primary focus at this stage was on validating customer dependencies and addressing scope and timelines.

   d. Stage 4: This was the Fujitsu governance approval process, led by the Assurance team.

   e. Stage 5: This was final approval of the replan by the Post Office.

52. In 2009 I was asked to become Programme Director, which was authorized by the Fujitsu Head of Core Services at the time, Peter Jeram.

Initial pilot problems

53. I do not recall the specific problems with the Horizon Online solution that arose during the initial pilots of Horizon Online, including any failures with the Systems Management Toolset. However, having seen an email that I sent dated 19 February 2010, I am reminded that there were a number of issues encountered with the deployment process which were resolved prior to going into the large scale pilot (WITN480_01/5).

54. I do recall that there were a number of defects going into the pilots which, I believe, would have been documented in a test report that was produced as part of the acceptance process. However, none of those defects were assessed as sufficient to stop the pilot. We would have assessed those defects with the Post Office for potential business impact and technical impact, and agreed workarounds where required.

55. Incidents were raised through the service desk for any issues encountered in the pilot. Where the resolution required a code fix, this would be passed to 4th line support where a defect would be raised and tagged to the incident. The defect would be annotated with the cause of the defect and the resolution. I suggest that the incident system be searched for any ticket raised by a pilot site that has a corresponding defect number to identify technical issues raised during the pilot phase.

Suspension of high volume pilot

56. Shortly after the high volume pilot commenced, a substantial number of branches in the pilot reported that the Horizon Online counter had "lost connectivity" and so they

were not able to trade. This issue would recur about two or three times a week, impacting a significant number of post offices in the pilot, and it would last about 10 to 20 minutes.

57. There was an intermittent issue encountered where the Branch Data Base locked, which stopped communications between the central database and the branch, so no transactions were able to be processed at the impacted pilot offices. As such, the high volume pilot was extended until the issue was resolved. After assessment, we quickly traced it to the Oracle code in use on Horizon Online.

58. An incident was raised against Oracle and we initially had to demonstrate that it was not an issue with the way we had implemented the solution. Oracle provided us with enhanced diagnostic tools and we fed diagnostic data back to them. We also had Oracle consultants from the Netherlands and the United States fly in to look into the issue. I also invited James Stinchcombe, an employee of Fujitsu though not working on Horizon Online at the time, to review the issue due to his knowledge of the Horizon architecture.

59. Once Oracle accepted that the fault was in their code they provided a technical patch to fix the issue within a week. The patch tested positively in terms of resolving the issue. There is a very technical explanation on why the patch worked, and I do not understand it fully. Even though the patch worked, we undertook a full regression test to ensure that we did not break anything else on Horizon Online by adding the patch. We then applied the patch to the pilot Post Office branches and we monitored the outcomes with the Post Office. It took about 8 weeks from the incident first occurring

to the patch being deployed. The patch operated for four weeks in the live pilot, during which time there were no repeats of the Oracle issue.

60. At the conclusion of the pilot phase, a report titled ‘Acceptance Report for HNG-X Acceptance Gateway 4’ (WITN480_01/11) was prepared to document how the Horizon Online system had met the relevant acceptance criteria and to support approval to move into the deployment phase. This report was presented to the Acceptance Board, which met on 29 June 2010 and approved the deployment of Horizon Online. I reviewed both the Acceptance Report for HNG-X Acceptance Gateway 4 and the minutes of the acceptance board meeting on 29 June 2010 (which provides details of the meeting, including attendees) (WITN480_01/12:) to refresh my memory of these events.

GENERAL OBSERVATIONS REGARDING SYSTEM REQUIREMENTS AND DESIGN

61. My understanding was that the requirements for the Horizon system were set by the Joint Authority (i.e. Post Office and the Benefits Agency) or, after the Benefits Agency’s involvement ended, the Post Office. These requirements formed part of the contract that ICL Pathway or Fujitsu had to deliver. ICL Pathway/Fujitsu were responsible for producing design specifications and had to demonstrate that they met the requirements in the Horizon contract. These specifications were subject to approval by the Joint Authority or the Post Office (as applicable).

62. The process followed for producing design specifications was that there were a number of high level requirements specification documents produced by ICL Pathway subject matter experts. These documents extracted the requirements from the various contract schedules into a single source specific to different areas of the

solution. These documents outlined how the Horizon Solution would meet the contractual requirements applicable to that area. The two documents applicable to my security work stream were the Security Functional Specification and the Access Control Policy, with an additional document, Requirements for Key Management (WITN480_1/13), that was not specific to contractual requirements. These documents were reviewed by ICL Pathway and the Joint Authority. Reviewers would submit comments on a template provided with the document. The document author is required to resolve all comments submitted through the review process and agreeing resolution with reviewers prior to submitting the document for approval. The document approver is responsible for assuring that all comments received through the document review process have been satisfactorily addressed prior to approving the document. Technical designs would then be produced to conform to the requirement specification documents and these went through the same review and approval process. This process was used for both Horizon and HNG-X.

<u>ASSESSMENT OF CERTAIN ASPECTS OF THE HORIZON SYSTEM AND DEVELOPMENT PROCESS</u>

<u>Robustness</u>

63. As a preliminary point, I note that I was not involved in the Horizon IT system throughout its life, and so I am only able assess its robustness[1] from the perspective

[1] Defined by the Inquiry as including: "*(a) the accuracy and integrity of the data recorded and processed by the Horizon IT System (b) the extent to which deficiencies in the Horizon IT System were capable of causing and / or caused apparent discrepancies or shortfalls in the branch accounts (c) the ability of the Horizon IT System to identify errors in data and discrepancies or shortfalls in branch accounts and the cause of the same and (d) the ability of the Horizon IT System to continue to operate satisfactorily in the presence of adverse conditions.*"

of the roles I held during the periods of time I held them (as listed at paragraph 6 above).

64. During my involvement, which included some time prior to the national rollout as well as and during the development and rollout of Horizon Online, I did not have concerns regarding the robustness of the Horizon IT system. As is typical of any large and complex IT system, defects did occur. However, in my experience, these were fully visible to the customer (whether Post Office or the Joint Authority) and, where required, agreed workarounds were put in place. I cannot comment on the matters that may have been communicated to the Government, as I would not have been involved in any such discussions

Interaction between teams

65. During the period of time prior to the national rollout of Horizon, I led the Security Delivery Team. This team was part of the Delivery Organisation that was headed up by Terry Austin. I reported into the Release Programme Managers for the deliveries appropriate to each of the releases (e.g. Releases 1A, 1B, 1C). I am unable to recall the Release Programme Managers, save that I recall reporting into Martyn Hughes for a period of time in relation to New Release 2.

66. During my involvement with Horizon Online, I was the Programme Director accountable for all solution delivery team, including Applications, Infrastructure, Integration, Test & Validation and Deployment. I reported to the Post Office Business Unit Director, Gavin Bounds.

67. I believe there was sufficient interaction between teams in both my assignments. In the period prior to the rollout of Horizon, and while I was working on the KMS, my

team members and I were represented at the appropriate governance forums and were generally included as reviewers for documents applicable to our area of responsibility. For HNG-X, as part of my responsibilities as Programme Director, I put in place a Governance Framework. This Framework detailed key roles and responsibilities, the governance forums to be operated and the required attendees. The purpose of the Governance Framework was to outline what information is reported to whom, the purpose of regular forums, the attendees at forums and the decisions to be taken at each forum. I recall capturing this in a document to ensure that everyone understood their responsibilities and the decision-making structure of the project. The document also set out the requirement for work stream leads to establish an appropriate team meeting structure to ensure relevant information was disseminated. I would attend, on an ad hoc basis, team level meetings to satisfy myself that these were in place.

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated: 09/08/2022

INDEX TO THE FIRST WITNESS STATEMENT OF ALAN D’ALVAREZ

Exhibit Number	Description	Date	Inquiry Reference / Control Number	URN
WITN480_01/1	Key Management High Level Design	10 March 1999	POINQ0104325F	FUJ00098154
WITN480_01/2	Access Control Policy	24 February 1998	POINQ0094160F	FUJ00087989
WITN480_01/3	Security Functional Specification Document	12 May 1999	POINQ0094173F	FUJ00088002
WITN480_01/4	Pathway Security Policy	8 October 1996	POINQ0104324F	FUJ00098153
WITN480_01/5	Email from Alan D’Alvarez dated 19 Feb 2010 at 10.04am	19 February 2010	POINQ0104339F	FUJ00098168
WITN480_01/6	Minutes of ICL/Utimaco Meeting – BRA01 05.11.98	5 November 1998	POINQ0067977F	FUJ00078389
WITN480_01/7	PinICL PC0005088	24 September 1997	POINQ0109648F	FUJ00103477
WITN480_01/8	Exception plan for delivering KMS within current CSR+ timescales	Undated	POINQ0067452F	FUJ00077864
WITN480_01/9	Requirements for KMS at CSR+”	Undated	POINQ0123666F	FUJ00117495
WITN480_01/10	ICL Pathway Change Proposal No. 1987	17 May 1999	POINQ0123667F	FUJ00117496
WITN480_01/11	Acceptance Report for HNG-X Acceptance Gateway 4	7 July 2010	POL-0030035	POL00033100
WITN480_01/12	Horizon Next Generation	29 June 2010	POINQ0103331F	FUJ00097160

	Acceptance Gateway 4 – Joint Board Meeting no AG4-01			
WITN480_01/13	Requirements for Key Management	20 April 1999	POINQ0123662F	FUJ00117491