Witness Name: David McDonnell

Statement No.: WITN0062_01

Exhibits: WITN0062_01/1 to
WITN0062_01/5

Dated: 3 November 2022

POST OFFICE HORIZON IT INQUIRY

____

FIRST WITNESS STATEMENT OF DAVID MCDONNELL

____

I, MR DAVID MCDONNELL, will say as follows:

INTRODUCTION

1. I am a former sub-contractor of ICL Pathway and held the position of deputy development manager and then development manager of the EPOS Counter 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 24.10.2022 (the "**Request**").

PROFESSIONAL BACKGROUND

3. I completed a BSc Hons in Computer Science at Sheffield Polytechnic in 1987. I then spent over 11 years working as a software engineer and then development manager, starting with 3 years or so at ICL Bracknell.
4. I would characterise the IT industry at this time as expanding and maturing rapidly, which caused the industry to move away from mathematicians,

physicists and qualified computer science graduates. This was accelerated by the proliferation of agencies who pushed into the middle and only cared about the body count and not the quality of the hires.

RECRUITMENT BY ICL PATHWAY

5. I was hired by ICL Pathway on a contract basis around Easter time of 1998 by Mr Chris Humphries (full time permanent employee of ICL Pathway) who was development departmental manager and assigned as deputy development manager under Steve Warwick (development manager - contractor). Chris Humphries reported to Terry Austin (contractor) the program manager.
6. My recruitment interview was several hours long, 1-to-1 with Chris Humphries during which he expressed several deep concerns over the quality of the EPOS team and the code being produced. The interview took on more of a nature of management discussion on how to fix such a problem. Upon my recruitment, I was instructed to work on the EPOS Counter component of the Horizon system.
7. The team comprised Steve Warwick as Project Manager, 8 or so developers and 1 technical assistant, Brian Orzell. Initially after starting for ICL Pathway, I reported to Steve Warwick daily and to Chris Humphries weekly, plus the project meetings with Terry Austin. I worked at ICL Pathway for 2 years or so.
8. Within days of starting it became very obvious that:-
    a. Steve Warwick had immense knowledge of how the post office worked but was not technical and had no formal qualifications in software development.

b. There were no development standards or methodology, coding practices, peer reviews, unit testing standards, design specifications in place. In fact this team was like the wild west.

c. Several of the development team were not capable of producing professional code.

9. It was a company wide well known fact that there were several thousand outstanding bugs in the EPOS system. The team was the joke of the building. This was known up to the highest level including Fujitsu Japan because they sent over 3 coders to perform an audit.

THE HORIZON IT SYSTEM

10. At the point I was recruited to join ICL Pathway, I understood that it was a Government PFI, the Labour government flagship. It had been through some turbulent times and was in trouble. When I joined, the Horizon project was in final development and still under testing.

11. I set out the concerns I had with the development of the Horizon system in the report I co-authored, 'Report on the EPOSS PinICL Task Force (Ref: IA/REP/008) (WITN0062_01/1: FUJ00080690). These concerns were based on personal professional observations and the opinions of most of the rest of the building, some 200+ people.

12. I understood the underlying cause of concerns to be that the bid had been won using a prototype which had then been further developed upon instead of starting afresh properly. Additionally, there had been a lack of formalised, signed-off designs, a lack of discipline, a lack of professional qualifications in

key positions, a total disengagement of the chief architect Gareth Jenkins, poor coding standards, no methodology in place and no unit testing. The issues were critical, making the product unstable and were known to everyone in the building.

INITIAL ASSESSMENT

13. The impression I formed of the management of the project and the professionalism of those working on the project in the very early stages of my employment at ICL Pathway was that some were good and cared, and were trying to remedy concerns, and some were only there to align politically and fill their pockets.
14. I spent several weeks auditing the code, working with team members to understand their views and concerns if any, listened to as many people on the project as possible in order to ascertain where the problem lay. Once I had an understanding I tried to engage the management and chief architect and get them to understand the gravity of the situation in emails, verbal conversations and telephone calls.
15. The cause of the concerns about the Horizon system are set out in the report I co-authored, (WITN0062_01/1; FUJ00080690) which was produced as a result of the task force initiative.
16. I also requested access to a copy of the design specification and all existing documentation for the EPOS system. I did this because it's the starting point of all engineering – it sets out what you are trying to build. It is also important in managing and meeting the client's expectations and demands. Some of this

documentation was located and I was given access to that, but it was totally out of date.

17. I was able to glean that ICL Pathway had secured the award of the contract prior to my involvement through use of a rapid prototype demo. Upon securing the award of the contract, I would have expected ICL Pathway to produce a signed-off design, define a methodology and set of processes for every step of the design, development and acceptance process, ensure these were adhered to, put in place qualified persons at all levels and ensure they are all following the agreed processes. I was not around at the time of the procurement or early design stage and so am unable to comment on how this was done. I can only say that I heard they took the prototype and built on top of it. Looking at the code I would say that this is evident.

18. So far as I was aware, ICL Pathway had in fact dived in and progressed the prototype into development with no structures or process around it. This approach is fatal in a large project with several integrations. The client was allowed to scope creep and retroactively add to and change the requirements which was accommodated by Steve Warwick. The developers had no agreed path, plan or process to follow and so everyone did it their own way. There is a methodology called "Rapid prototyping" which used to be used to establish requirements and design, but building out a full build project on top of a skeleton prototype, which does not have the design and engineering foundations in place, is always going to lead to a confused outcome. Prototypes are built to learn what works and what doesn't, what is required and what isn't, what the client wants and what he doesn't. It is not usually intended that the basic prototype framework is ever used as the basis for the

main build out. There has since been the evolution of the “Rapid prototyping” methodology into something called “Agile”. Agile was not around in the UK in 1998 and was certainly not used on the Pathway project. Agile, despite its name, has a strict set of rules and processes none of which were used and in fact the most important word in Agile is discipline which was certainly not present.

19. Upon completing my initial assessment of the system, I concluded that 70% of it could be saved, fixed and tidied up, 20% needed a lot more work but could be kept, but that the critical Cash Account module was beyond repair and must be re-written. There was a layer of design missing from the EPOS system which would ensure only validated messages could be written to the message store. There should have been an Application Programming Interface layer between the code and the message store which ensured that only correct and validated messages could be written to the riposte message store instead of the freestyle that was currently allowed. This freestyle was like having a graffiti wall instead of a library with the Dewey system. Instead of each module reading and writing messages to the message store in a freestyle manner they should talk only to this Application Programming Interface which would only accept and reply to strictly controlled, documented and audited read/write requests and it itself would read and write the messages to and from the message store. This way only messages that were structured correctly and had valid content as set out in the data dictionary specification could be written to the message store.

20. In fact the message store often contained hundreds of junk, debug or test messages from different modules.

21. It was also possible for anyone to read and write anything into a message and post it to the message store outside of the EPOS modules. This was as technique used on occasion by the support team to correct erroneous cash balances.

22. I reported my conclusions to the following people:

    a. Steve Warwick, who ducked and dived and swerved the issue;

    b. Chris Humphries, who agreed and tried to influence change but was blocked by Terry Austin and higher levels;

    c. Terry Austin, who blatantly refused to allow it to be re-written;

    d. Gareth Jenkins, who denied the issues point-blank, ran off to hide in Bracknell and avoided contact with the team.

23. After some weeks of raising my concerns to Steve Warwick and Chris Humphries and trying to work with Steve Warwick and the team my views came to a watershed moment when Steve Warwick left for a 3-week vacation. During this time there were a number of category A serious defects that came up regarding the Cash Account module which was renown for being flaky. I finally had the opportunity to get Terry Austin to understand the gravity of the situation. This conversation gave rise to the "Task Force" initiative with myself and Jan Holmes in charge and which led to the document (WITN0062_01/1; FUJ00080690) being produced.

24. I managed to instigate the Task Force which repaired 70% of the system and got another 20% under repair. During this time, I co-authored document (WITN0062_01/1; FUJ00080690) - a report to all management detailing the issues and concerns with recommendations. I built a test unit inside the dev team staffed by a good test resource. I made the developers responsible for

their code and resultant bugs and I brought in development rollout plans and methodologies. I put change and release management software (Product Change Management System, a branded software control system) in place to track the releases and bug fixes, and insisted on documenting bug fixes and including these in a formal release note for each software release we did. I also fired some people and hired some people.

25. At the end of the Task Force (several weeks) we had fixed or aged out maybe 70% of the bugs but having studied the code and the message store beneath it I made 2 further recommendations:-

    a. The design of the system was missing a layer. There should have been an Application Programming Interface layer between the code and the message store, which I explain in paragraph 19, above. I fought hard to get Terry Austin and Gareth Jenkins (chief architect) to understand and agree to this. Terry Austin refused to allow this on cost and time basis and Gareth Jenkins refused to accept this for reasons that he never made clear. From this point on we made several attempts to get Gareth Jenkins to engage with the team and the problem and to lend his support to improving the quality etc but he merely became more and more evasive and unavailable. Without his backing I was unable to convince Terry Austin.

    b. At the very least the cash account module needed to be re-written which was not a big job. I estimated 6 weeks to complete.

The difference between my initial findings and those after the Task Force, was confirmation that the Cash Account needed to be re-written. I had been able to use some of the task force time and resource to confirm this with professional and qualified opinion from independent developers from another team.

26. I argued for a re-write of the cash account with Chris Humphries, who agreed, and also with Terry Austin, who refused. Instead he moved me out of the EPOS team (see paragraph 39) replacing me with Phil Hemmingway, who put the system live under Terry Austin's instruction.

27. At the end of the Task Force period Terry Austin had decided on a company reshuffle and I was called to his office where he asked me to formally take over as development manager of the EPOS team. I said I would accept on the one condition that we re-write the Cash Account module and assured him it was a relatively straight forward task, no more than 6 weeks. He became extremely irritated and the meeting came to a swift close.

28. The next thing I knew Terry Austin had appointed Phil Hemmingway as development manager of the EPOS team. Phil Hemmingway was a contractor and long-time associate of Terry Austin. Phil Hemmingway had worked for me as a business analyst during the Task Force. To my knowledge Phil Hemmingway had no formal qualifications in software engineering or design and it became clear that his role was to get it rolled out of the door as is with no questions asked. THIS IS THE MOMENT THAT THE DISASTER BECAME UNNAVOIDABLE.

29. I was moved off to manage a small self contained EPOS Logistics Feeder Service project which was done with zero defects at point of going live.

30. At this point in time and as a result of the reshuffle, all of the project teams in the building worked out that this was now a fait accompli, this was no longer a serious project and there was little point in speaking out. The culture changed

to "fill your pockets lads", a smash and grab trolley dash before it came to an end.

EPOS COUNTER SYSTEM

31. The EPOS Counter System is the Electronic Point of Sale; it's the touch-screen interface that the Post Office staff use to sell all the products through. All EPOS modules read and wrote messages into the message store, allowing them to be audited and picked up by other modules.
32. In terms of the establishment of the EPOSS PinICL Task Force (the "Task Force"), the PinICL system had always been in place and was administered by another team in the same building. During the Task Force the PINICL admin team assisted with managing and tracking the different stacks and producing reports and statistics on demand. Anne Croft was a member of this team.. They split the stacks into different categories so that we could manage the thousands of bugs more easily. The purpose of the Task Force was a 6-week blitz on the outstanding bugs. I was allowed to pick several team members from other teams to help and was given priority on all resource. We numbered maybe 20 in total with satellite help. Its purpose was to get the EPOS code into a good enough state to be able to move on in a managed way. At the outset of this, I was threatened with violence by an individual with a reputation for violence and who was a long-time associate of Terry Austin for taking his best 2 people into the Task Force.
33. Everybody on the Task Force was actually enthusiastic and happy to see that finally something was getting done. Some on the periphery were sceptical, but

mostly we were well supported. Everyone worked really hard for 6 weeks, long hours and good commitment. I consider the Task Force was successful in meeting its objectives, with the exception of the Cash Account.

34. In Autumn 1998, I considered that the EPOSS product, its code and design, was better than it had been 6 months previously. The code quality being released was better. The number of critical bugs being raised was way down and manageable due to it now being tested before it left and expectations being higher and processes in place. The release process was also now very good but the Cash Account was still broken.

35. I attributed the deficiencies in the EPOS product to poor and unqualified middle and senior management, most of whom had little interest in following a proper design and development lifecycle, fixing issues, had limited or no technical skills that I saw and who only played the politics and pushed for a deadline. There was a failure to implement proper development lifecycles processes, such as development methodologies, coding standards and the absence of design documents. By 'middle and senior management, I refer to Terry Austin, Mike Coombs, Gareth Jenkins – those in my direct line of interest in the EPOS side. The other management on other lines were also aware. These are the people who were responsible for hiring the right people and putting all these quality assurance processes in place. If you're a coder in the trenches and you're told to do something, you get on and do it, it is very difficult to change a whole culture from this level. The developers should be there to code and be free to adhere to professional standards supported by middle and senior management. The project and program managers should

be the ones ensuring that those standards are in place, understood and adhered to.

36. I have been referred to the Report, document (WITN0062_01/1; FUJ00080690), and specifically the “PinICL fixing culture”. In the absence of a design, the joke was that PinICL no.1 was “There is no system.”, the fix being “Build a system.” etc. Instead of a PinICL being raised which referred to a signed-off design specification as the golden source, they often expressed opinion, preference or even new features.

37. I have also been referred to the term “code decay”, also in (WITN0062_01/1; FUJ00080690). Code decay can occur and evolve in many ways. When a piece of software is written against a specification, it should be clean and clear and comply with the design, easy to read, with changes being well documented and auditable. In many EPOS cases code was changed without any audit trail, it would cause it to become unreadable and often contradictory spaghetti. With no coding standards to comply to, no peer reviews and no accountability, there was a total lack of discipline.

38. In Autumn 1998, I told Gareth Jenkins, Terry Austin, Chris Humphries, Phil Hemmingway, Steve Warwick and many others several times that the Cash Account must be rewritten. I also wrote the report referred to above and sent several emails. This resulted in me being moved from the EPOS team for my noise. In particular, I raised my concerns with the following people:

    a. Chris Humphries, who agreed but was blocked;

    b. Terry Austin, who got angry, removed me from the team and moved me elsewhere;

    c. Phil Hemmingway, who agreed in private but put it live anyway.

39. As a result of the concerns I had raised and for insisting on a re-write I was moved out of the way for not saying the right answer. Phil Hemmingway replaced me.

40. ICL's parent company, Fujitsu, sent an audit team of 2 or 3 developers from Japan to audit the code. I showed them where it was and what I thought. They worked for 2 days or so looking and then disappeared.

41. I have observed several witness testimonies referring to the proposed "re-write" as a big deal, a big job that could potentially introduce more problems than it would fix. This was not necessarily true and indicates either a basic misunderstanding of how the EPOSS system was built or even potentially suggests an attempt to obfuscate the issue. The EPOSS system was modular and what the other engineers and I were proposing as an immediate action was a re-write of ONLY the cash account module. It would have been possible to write a new, second version of this module alone leaving all of the other code untouched. As this module was a batch job usually run out of hours it did not interact with the other modules in the system and therefore there would have been almost zero chance of it causing any regression to the other parts of the system. It would even have been possible to have a second "shadow" cash account run alongside the original on the counters in order to prove it worked before jumping horses onto the new one. This would have mitigated almost any risk of regression. This work we estimated could have been done in maybe as little as 6 weeks or so. It could have been done as a standalone piece of work without interfering with any of the other EPOSS development. It would have then been possible to follow on by rewriting any other modules we felt necessary 1 at a time if required. Had we been allowed

to do this I am certain that we would not be here today. At no point was anyone proposing we re-write the whole system from scratch in one go. Having re-read the initial task force report (WITN0062_01/1; FUJ00080690) I do not think that this was made clear in this initial document itself but it was made very clear in the recommendations which followed as well as all of the conversations we had when trying to convince management that this was the only course of action.

42. I would add that given EPOSS was primarily a financial accounting system then the priority should have been given to ensuring that the cash account was accurate and reliable. If the system was slow or occasionally blue screened or suffered from other non critical defects then although the users may have been inconvenienced at least they would not be getting prosecuted.

43. I would like to state that there were no diagnostic tools provided by Escher or built in house which enabled L1,2,3 support or even the developers to trace and diagnose issues with the cash account balancing. This is evidenced by Pinicl WITN0062_01/5; FUJ00067416 which clearly demonstrates the team's inability to trace any fault in the accounting. This was probably one of the biggest deficiencies in the design in my view and I asked several times to be allowed the time and resource to build something but was told no

REASSIGNMENT

44. I did not remain assigned to the EPOS Counter System on completion of the Task Force, I was moved out to lead the Logistics Feeder Service team then AWS after Logistics Feeder Service went live with no issues. In each case I

was moved by Terry Austin, to the LFS team and then AWS team after I put the LFS system into final test and pre-release. I consider the reason for my reassignment was that I refused to put the system live in the state it was.

45. Phil Hemmingway was responsible for ongoing development of the EPOS Counter System after September 1998 under Terry Austin.

46. I had a small team of 2 really good guys in the Logistics Feeder Service. We had a great design document from Vin Patel. I did a small amount of development work in C++ then mostly project management and release management work. Then I was moved up to the AWS team.

47. I did not have any concerns about the Logistics Feeder Service. I did have concerns about the AWS. This was managed by Steve Doyle. It was mostly a pretty good, well written system, but when I was ordered by Steve Doyle to release a new version of the software that was not complete and had known bugs, in order to meet a deadline, I refused. Shortly after this I was replaced by a staffer from Bracknell called Nick Lawson (although I'm not sure of his last name). Then I left the company.

CORE SYSTEMS RELEASE PLUS (CSR+)

48. I have been referred to documents (WITN0062_01/2; FUJ00079782), (WITN0062_01/3; FUJ00079783) and (WITN0062_01/4; WITN04600104). I did not have any involvement in the development audit of CSR+ and/or in the production of the Report on EPOSS Solutions dated 21 September 1999. They were all done by Jan Holmes who was my partner in the Task Force and produced these as a result of everything we learned during the Task Force

and after. I may have answered some questions for him or contributed verbally.

49. I was indirectly responsible for the recommendations made in this report to re-design and re-write EPOSS (WITN0062_01/3; FUJ00079783). This conclusion was drawn from the work Jan Holmes and I did in 1998. I was consulted verbally and my recommendations hadn't changed. This was a year later and by then I had moved to AWS. Jan Holmes authored this report and made these recommendations in September 1999.

50. In respect of the decisions taken by the senior management within ICL Pathway upon receipt of these recommendations, I did not witness this first hand but was told by several who did that Peter Mandelson, the Trade and Industry Secretary, had been in the building again and made it clear it had to meet the deadlines or Blair would not be happy so Terry Austin and Mike Coombs were pushing it out regardless.

RELATIONSHIP BETWEEN POST OFFICE COUNTERS LIMITED, THE GOVERNMENT AND ICL PATHWAY

51. I witnessed the liaison between representatives of Post Office Counters Limited and ICL Pathway during the design and development of the Horizon system daily, between Steve Warwick and a POCL lady. The discourse and interaction was always very good. Post Office Counters Limited had a presence in the building and POCL and ICL Pathway met almost daily. I attended some of these meetings. I understood that the POCL rep Barbara Longley was in attendance and Steve Warwick mostly from ICL Pathway.

52. POCL knew that there were problems with EPOSS and particularly around the Cash Account but I think Pathway did a good job of screening it so they never knew just how many bugs were outstanding. They did know the Cash Account didn't work as evidenced by the PinICL document shown to Terry Austin by the Inquiry when he gave oral evidence on 27 October 2022. This is document (WITN0062_01/5; FUJ00067416).

53. In terms of the extent to which POCL were involved in the testing of the Horizon IT system, they did acceptance testing but it was more around the look and feel and features rather than resilience testing or deep dive testing. I understood the representatives of POCL from their oversight of testing were generally happy with the look, feel and features. I don't know if they ever tested the Cash Account.

54. During my time at ICL Pathway, I saw Peter Mandelson twice in the building but did not attend the meetings. I was told by someone who was there that he said it has to go live and they told him what he wanted to hear.

TERMINATION OF EMPLOYMENT WITH ICL PATHWAY

55. Whilst working for Steve Doyle in the AWS team, I was instructed to release a piece of software that was not complete, untested and had known bugs. I refused and shortly after I was replaced by an ICL permanent member of staff from Bracknell – Nick Lawson (I am not sure of the last name). After my time with ICL Pathway, I moved to another job with CSC developing Thames Water billing system followed by 2 years in Tokyo with Merryll Lynch on their equities and derivative trading floor. In the years after leaving ICL Pathway, I

worked mostly in the banking industry on financial systems, trading floors, equities and derivative trading/wealth management systems in Paris, London and Switzerland for tier 1 institutions such as Santander, Credit Suisse, Natixis and UBS.

THE UNFOLDING SCANDAL

56. I became aware of the unfolding Horizon scandal the day I joined. Then after it went live I was living abroad so first heard that the post office were prosecuting people through Private Eye magazine. RO RO

57. My actions during my time there are previously documented. Outside of my time there and outside of the project, I RO advised a QC Barrister who was representing a client on a murder charge where the main thrust of prosecution case was that he stole money from the EPOS counter which was his main motive for the crime. RO RO

Statement of Truth

I believe the content of this statement to be true.

Signed: GRO

Dated: 3 November 2022

Index to First Witness Statement of Mr David McDonnell

No.	**Exhibit Number**	**Document Description**	**Control Number**	**URN**
1	WITN0062_01/1	Report on the EPOSS PinICL Task Force (Ref: IA/REP/008)	POINQ0086861F	FUJ00080690
2	WITN0062_01/2	ICL Pathway CSR+ Development Audit v1 dated 28/10/99 (Ref: IA/REP/015)	POINQ0085953F	FUJ00079782
3	WITN0062_01/3	ICL Pathway Schedule of Corrective Actions re CSR+ Development Audit dated 22/11/99 (Ref: IA/CAP/008)	POINQ0085954F	FUJ00079783
4	WITN0062_01/4	ICL Pathway Schedule of Corrective Actions: CSR+ Development Audit v2.0 dated 10/05/00 (Ref: IA/CAP/008)		WITN04600104
5	WITN0062_01/5	Error Log PC0045061	POINQ0075856F	FUJ00067416