WITN04190200

WITNESS: TERENCE PAUL AUSTIN

WITNESS STATEMENT: WITN04190200

DATE SIGNED: 19 July 2024

POST OFFICE HORIZON IT INQUIRY

SECOND WITNESS STATEMENT OF TERENCE PAUL AUSTIN

I, Mr Terence Paul Austin, will say as follows:

INTRODUCTION

1. Following on from my first written statement dated 13 September 2022 and oral evidence given to the inquiry on 27th October 2022, I would like to provide an additional statement which aims to clarify some of the assumptions made and conclusions drawn during Phase 2 and subsequent phases of the Inquiry.
2. This statement is provided in response to the Rule 9 Request number 1 dated 7 June 2022 for information pursuant to Phase 2 of Inquiry: Horizon IT System: procurement, design, pilot, roll out and modifications.

UK GOVERNMENT IT SYSTEMS

3. During the 30-year period from the late eighties, the number of UK Government sponsored IT systems which failed was significant and well documented. A few examples are as follows:

   Child Support System

WITN04190200

Passport Automation System

Magistrates Courts System

Centralised NHS System

E-Borders System

Army Recruitment System

Universal Credit System

Benefits Card System*

Farmers Rural Payment System

4. All the major IT hardware and software companies throughout the world were involved at some stage in the development of these systems, and the long list demonstrates that in many cases the UK Government did not possess sufficient managerial or technical expertise to ensure successful delivery. In the case of Horizon, adopting the PFI approach was entirely inappropriate for a large, complex IT system and this was compounded by the fact that the DSS/POCL management team did not understand how this changed the engagement process between the supplier and the customer. Although this had an enormous impact on the delivery schedule, the Horizon system was one of only a handful of systems in the nineties which managed to achieve formal customer acceptance and was successfully rolled out, despite the appalling history of government ineptitude.

5. With the benefit of hindsight, there was an enormous gap between the what the ICL bid team believed they were being asked to deliver and the

WITN04190200

expectations of the DSS/POCL procurement team. Fundamentally, there were two ways that an IT system could be procured in the nineties, a suitable analogy is the process involved in buying a house. One can either a) buy a house which has already been designed and built to a predefined specification for a specified price or b) commission an architect/builder to build a house to your specification for an agreed price and timescale. In either case, any subsequent changes/additions would be delivered for an additional cost. To appreciate the gap in understanding between the ICL Pathway bid team and DSS/POCL is that ICL thought that they were dealing with option a) above (i.e. an off-the-shelf IT solution) but DSS/POCL assumed they were working with option b) above, so the two parties were polls apart. The subsequent position papers by both parties demonstrated this, see **[POL00031117]** and **[POL00038829]**.

6. There are numerous references in documents shown to the Inquiry claiming that ICL Pathway underestimating the size of the task, and this was the cause for the delays. I indicated in my first statement that during the bid phase, there was no detailed functional specification produced by either the Benefits Agency or Post Office Counters Ltd, there was only a high-level list of requirements which could be satisfied by a variety of architectural and functional solutions. The solution submitted by the ICL Pathway bid team was based on EPOS software initially developed for the Irish Post Office and enhanced to incorporate benefits payment functionality. The delivery schedule was based on this system and the only additional work required at that time was to develop a few small counter applications and a mechanism to interface with the customer's IT systems.

WITN04190200

ICL Pathway was predominantly an integration team i.e. one which pulled together systems from several other third parties and provided the software glue that enabled them to operate as one homogeneous solution. This system was demonstrated to DSS/POCL personnel on many occasions during the bid phase and it was clear that this was the solution that ICL Pathway would deliver if it was awarded the contract. One of the highest risks on the ICL Pathway risk register at this time was that the functionality being provided could subsequently be rejected by DSS/POCL because the list of requirements was defined at such a high level that they were susceptible to misinterpretation, opinion and subjectivity. So in an attempt to mitigate this risk, a detailed functional specification of the ICL Pathway solution was produced and a clause included in the contract which stated that this specification must be signed off by DSS/POCL within 30 days of the award of the contract. This was never achieved so to all intents and purposes; DSS/POCL were in breach of contract. Another high risk was that several critically important facets of the system had not yet been specified by the DSS/POCL e.g. Security and Audit requirements. These became known as ‘Agreements to Agree’ which was a strange concept because once the requirement had eventually been written down and approved, additional software would have to be developed resulting in further cost and delays, which is exactly what happened. Effectively, the system functionality would be incomplete and not operationally viable in the first few releases of the system and there was no timeframe when these elements would be developed.

WITN04190200

7. What all this demonstrates is that DSS/POCL expected the supplier to submit a fixed price and timescale for a detailed requirement yet to be specified, a nonsensical expectation and totally at odds with PFI principle that the supplier provides a packaged solution at their cost and recoups their investment during the live operational phase. Consequently, any unforeseen costs or delays during the development stage would impact the level of revenue the supplier could achieve later. The financial risk rests entirely with the supplier, and it was for this reason that ICL Pathway would not allow DSS/POCL to interfere with the development process or enhance their functional requirement without a change control process. Effectively it was originally a fixed price contract to deliver a customer signed off business solution within a specified timeframe. A failure by the customer teams to appreciate this from the start was the source of much of the tensions displayed by both parties during the development phase. It only became a true example of option b) - (see paragraph 3. above) when the Codified Agreement was signed by Post Office in July 1999 **[FUJ00000071],** i.e. 3 years after the contract had been awarded and only a few months before live trial was due to commence.

DSS BEHAVIOUR AND SUBSEQUENT WITHDRAWAL

8. The subsequent withdrawal of DSS from the contract has little relevance to the Horizon Inquiry other than to demonstrate that POCL were not equipped to manage or operate an IT system of this magnitude and explain why POCL was left to manage and fund the contract on their own. DSS had taken the lead right from the start and had considerably more experience with large IT systems. Therefore, it was with some surprise to

WITN04190200

encounter their unwillingness to engage productively at any stage, especially as the timescales for implementing the first release of the benefit payments functionality was only months away. I can only speculate with the benefit of hindsight, that this adversarial behaviour and lack of cooperation was either because they were a) unable to meet their contractual obligations leaving themselves open to legal challenge or b) they had concluded that using the post office network to administer benefit payments was an expensive option and preferred the 'social inclusion' option which ensured that every beneficiary was able to open a bank account and be paid by bank transfer. The official reason was that delays to the programme had eroded their business case but in reality, they had been instrumental in orchestrating this.

9. Whatever their motives, they would have to find politically acceptable and financially neutral way of withdrawing from the contract. To do this, they tried to claim that ICL Pathway had a) not delivered the benefit payment functionality requested, b) fallen short on the security requirements and c) not provided the correct data to their IT systems. I believe that they were also implying that there were issues with data integrity and software reliability but the evidence from the live trials did not support these claims. If their action had been successful, it would have resulted in ICL Pathway writing off millions of pounds in costs. Their action failed because a) they had not signed off the business functional specification within 30 days as required and were therefore in breach of contract, b) the Security Requirement was an 'agreement to agree' and had not yet been specified by the DSS and c) they had not provided the data interface specifications

WITN04190200

for their systems as requested by ICL Pathway. ICL Pathway then counterclaimed for their sunk costs and loss of subsequent revenue for the Benefit Payments System (BPS) operate phase. The parties eventually decided to proceed on a 'no blame' basis and Government concluded they had no choice but to continue with the programme leaving POCL to pick up the cost but without the benefit of the DSS business. This has been mentioned several times in witness statements, in some instances referred to as the DSS/ICL 'stitch up' and was the reason for the initial bad feeling between POCL and ICL.

IT SYSTEM DEVELOPMENT

10. Most people outside the IT Industry have an expectation and perception that all IT systems are error free. Although this objective, known as 'zero defects' was always the goal to aspire to, it was to my knowledge, never achieved then, and is not achieved today. Every large IT system will contain errors for the first few years of its life, some of them serious but the actual number would depend on the size, complexity and category of the system involved.

11. It is for this reason that many of the large legacy IT systems are still running 20 years or more later because 99.9% of the glitches, defects and errors have been uncovered and fixed and the systems are now very reliable. Over time a new 'front end/user interface may have been developed to bring them up to date and other features enhanced to take advantage of the latest technology, but the core software remains the same. I am not able to say one way or the other whether the upgrade from Horizon Legacy to Horizon Online (HNGx) adopted this approach.

WITN04190200

12. The cost and timescales required to deliver a system is hugely influenced by the nature of the application. There are those which were categorised as *'administrative'* systems, example applications would be retail, banking, insurance, taxation, utility billing etc and those where the implications of a serious defect could be catastrophic and/or life-threatening. For example, applications managing air traffic control, transport signalling, space programmes, medical diagnostics/treatment, weapon systems etc. The systems that fell into the latter category would be subjected to considerably more testing and rigour, requiring far more resources and time to deliver. In some cases, the time taken would result in the system being technologically out-of-date by the time it went live. By this I mean obsolete and unsupportable without special arrangements with the suppliers because they were based on technical platforms which had since been superseded. If a system had been categorised in this way, all parties would have been aware of the additional cost and time implications and the associated risks right from the bid phase and this was definitely not the case with the Horizon system. An *'administrative'* system on the other hand would be subject to cost and time constraints otherwise they would be uneconomical to deliver. The original delivery timeframe indicated that Horizon was very much regarded as an *'administrative'* application, so it was inevitable that it would contain known and unknown software faults in the first few years of operation. Although the consequences of these faults would not be life threatening, they would nonetheless have serious financial implications for the organisations involved. Notable examples over the past 20 years were:

WITN04190200

US Brokerage Knight Capital 2012

NASDAQ Incident 2012

RBS System Crash 2015

HSBC Major outage 2016

TSB Migration Issue 2018

Wales NHS Patient Files Access Failure 2018

Heathrow Check-In System Failure 2020

13. As far as I can recall, I was never made aware of the fact that the IT system was to be used to prosecute and potentially imprison post office staff. Had I known that an accounting glitch could result in post office staff being prosecuted and imprisoned, I would have responded with incredulity and disbelief because the risks of a miscarriage of justice would be considerable. Had this expectation been made clear from the outset, the solution could no longer be considered an *'administrative'* system because the implications of a software fault were potentially catastrophic, so a different engineering approach would be required. The requirement to satisfy PACE was seen by my security and audit colleagues simply as a 'certification' procedure and not a requirement to produce fault free software. Personally, I could not see how the PACE criteria for admitting computer generated documents could ever be satisfied by a large complex system because one can never be 100% certain that there are no, as yet undetected errors in the data or the software, irrespective of how much testing the system is subjected to. I only learnt from the Inquiry that the

WITN04190200

requirement to supply audit data (ARQ) to support prosecutions only emerged 2 years or so after roll-out had commenced. All systems need time to settle down and any indication that a potential fraud had taken place should in my opinion always be corroborated by external evidence and/or manual processes. For example, even today the accepted wisdom given by industry observers is not to upgrade your personal PC to the next version of Windows for at least 12 months, to give it time to stabilise, and that's a version upgrade not an installation of a completely new system.

14. The ICL solution, prior to DSS withdrawing from the contract, included a comprehensive and sophisticated fraud investigation service based on an Oracle database. This enabled DSS to carry out 'deep dive' investigations into potential cases of fraud. I believe that his facility was offered to POCL but was rejected on cost grounds. If my memory serves me correctly, the audit data, that was provided on request from POCL, was raw i.e. it simply showed what transactions had been recorded at the Till and I would assume required considerable technical knowledge to interpret.

15. The nature and size of the post office network and the diversity in the capabilities of the end user, meant that one of two faults would not come to light for several years due the huge number of variables. In was not feasible to create laboratory tests which would prove conclusively that the system would operate perfectly in a network of 19,500 locations and 40,000 tills, no matter how extensive they were or how often they were executed. All that would be possible would be to model the different types of outlets in the network and simulate the transaction traffic. These tests were followed by a 'live trial' involving a limited number of post office

WITN04190200

outlets (circa 200) selected to ensure that all the different types were represented from small, isolated post offices up to multi-counter crown offices.

ICL PATHWAY TESTING

16. There has been considerable speculation surrounding the adequacy of the ICL Pathway testing strategy even though hundreds of skilled testers were involved, tens of thousands of hours expended, enormous volumes of documentation recorded, millions of pounds spent, and countless hardware/software platforms built and rebuilt. The approach was to slowly add layers of functionality and gradually build the solution until it became the complete system running in its live target environment. The objective is to uncover errors as early as possible in the testing cycle because it is much less time-consuming and costly to find them in the latter stages. Individual components of the solution would first be tested in isolation this was referred to as 'Unit Testing', then all the elements of a product/application would be assembled and tested, this was known as Link Testing. These early processes used a cut down version of the hardware configuration and were carried out by the programmers who developed the software. The next stages were more rigorous and involved specialist testing teams. Formal test scripts, plans and reports were written based on the customer's business 'requirements and the expected results would be documented. These functional tests would be enhanced as the system became larger and larger and more complex. The various stages were known as system testing, business integration testing, end to end testing, destructive testing (simulating irrational user behaviour), model

WITN04190200

post office testing, rehearsals and live trials. In addition to and running alongside these business functional tests, would be numerous technical tests designed to verify system performance, scalability, backup and recovery and the requirements associated with security, audit, data migration and archiving.

17. Finally, there was regression testing which was designed to test enhancements to the business functions and bug fixes, to confirm that these had not adversely impacted code and functionality which had already been tested successfully.

USER ACCEPTANCE PROCESS

18. Acceptance testing was a formal and independently managed process for verifying that the system had delivered all the business functionality and was performing in accordance with the technical requirements e.g. transaction response times, security, auditability, scalability etc . POCL's success/acceptance criteria was defined in document **[POL00029137]** and later revisions. To achieve this, each individual business requirement was extracted from every signed off specification document to create a 'Requirements Catalogue'. Each entry in the catalogue was then linked to the specific test and results which demonstrated that the requirement had been met. All the test scripts and the results were witnessed and signed off by BA/POCL personal. The entire process was overseen by PA Consulting who also acted as an independent arbiter in the event of a dispute. Each Director in ICL Pathway had different responsibilities and personal performance criteria, to ensured integrity and that no one 'marked their own homework'. The Requirements Director (John Dicks)

WITN04190200

and Security & Audit Director (Martyn Bennett) made sure that all the business requirements specified by the Benefits Agency and Post Office had been correctly reflected in the various specifications and in the requirements catalogue. These two Directorates would then support BA/POCL during the Acceptance process by investigating all acceptance incidents raised and would amend documentation if this was found to be inadequate or provide evidence to show that it was an end user error or prove that the system was performing as requested. My Directorate operated at arm's length and only became involved when it was necessary to amend the software and run witnessed tests to demonstrate that the fault had been fixed. BA/POCL made the final decision as to whether an incident had been resolved and should be closed.

19. In addition to the functionality provided by the software and hardware, 'Acceptance' also covered the service processes including new software releases, the help desk, 2nd, 3rd and 4th line support, performance monitoring, fallback and recovery and business continuity.

20. The acceptance umbrella also included the software methodology and engineering processes adopted to produce the solution. An independent third-party verified and certified that ICL Pathway had achieved the ISO 9001 standard required.

21. Finally, a mechanism was agreed to measure the 'robustness' of the system which involved the categorisation of software faults documented in the 'known error log (KEL)'. If I recall correctly, there were four priority categories, A, B, C & D and the acceptable number outstanding allowed for each was specified. The issue with this approach is that it cannot

WITN04190200

quantify faults which have yet to be discovered. Only time can do this, that is why I have said earlier in my statement that large complex systems can take 2 or 3 years before the majority of errors have been uncovered. Even then, 'sleepers' can exist which only emerge when a rare and complex set of circumstances and variables occur.

22. The Live trial was part of the Acceptance Process and the roll-out of Horizon did not commence until formal acceptance of the solution had been achieved. We did encounter balancing errors during live trial and POCL were well aware of these 'acceptance' incidents, and ICL Pathway had to provide evidence that these had been fixed. We were also closely monitoring help desk calls referred back to 4th line support to determine if there was any indication of a more fundamental issue

EPOSS FUNCTIONAL REQUIREMENTS

23. As stated earlier, the EPOS solution submitted as part of the ICL Pathway bid was based on the 'point of sale' application developed by Escher for the Irish Post Office. It was enhanced to include the benefit payment functionality required by DSS. So basically, it was an 'off-the-shelf' solution which was running successfully for An Post. The specification which described the functionality on offer was made available to DSS/POCL who were asked to approve within 30 days of award of contract. This they did not do, and we were given no explanation, however it did mean that they were potentially in breach of contract.

24. The first 12 months or more focussed on the benefit payment functionality (IGL) and the EPOS application was largely ignored. I cannot remember the exact sequence of events but at some point POCL informed us that

WITN04190200

EPOSS did not meet their requirements but accepted that they had not produced a detailed requirements specification. This presented the programme with a major problem because the delivery schedule could not accommodate a delay while waiting for POCL to document their requirements and then for us to develop the new software. We suggested that the only way forward in the circumstances was to use an emerging iterative/incremental methodology referred to as Rapid Application Development (RAD) or AGILE. There was no certainty that this would work, but it was worth the risk because the alternative was to bring the contract to a halt. I think that ICL Pathway and POCL were aware at this time that DSS intended to withdraw from the programme.

25. The RAD approach requires that the customer and the developer work closely together to incrementally build and test the software. I can't recall whether I initially outsourced this development to a third party or whether I recruited software developers with RAD experience to join the ICL Pathway team. As I have stated previously, ICL Pathway was an integrator and only had a small development team and finding people with the necessary RAD skills would not have been easy, so I suspect it was the former although I can't be certain. POCL and ICL knew that a detailed functional requirement for EPOSS was required for the acceptance process and the only method of producing this was to reverse engineer all the documents from the developed code. Not ideal but there was no other option.

EPOSS TESTING

WITN04190200

26. Once a third party had built an application, it would be subject to an ICL handover process including product acceptance testing. Following this, the counter PC would be assembled and enter system testing. I believe that it was at this stage that my testing team started to raise concerns about the quality of the EPOSS software.

27. It was becoming evident that the quality of the unit and link testing carried out by the developers left a lot to be desired, because many of the faults being detected by my team should have been identified and resolved long before the product was handed over.

28. In the summer of 1997, I was advised by my architects to ask one of our partners Escher (experts in Microsoft messaging technology) to review the code and re-engineer it if necessary. Following this, more functional changes were requested by POCL and a large number of bug fixes were applied. However, I was still receiving reports from our testing team that the number of issues being raised was unacceptably high. Consequently, in 1998 I formed a task force to investigate the root cause and devise a corrective action plan.

EPOSS CORRECTIVE ACTION PLAN

29. It has been suggested that I rejected the task force findings, this is not true and a ridiculous insinuation in the circumstances. EPOSS was critical to the success of the programme, consequently I took the recommendations very seriously indeed including the proposal that a complete or partial rewrite should be considered. I consulted with all my managers and technicians before deciding on the best way forward. A corrective action plan was put in place and many changes/improvements were

WITN04190200

implemented. The issues with unit and link testing were addressed along with the quality of the documentation. We took control of the development activities and populated the team with more experienced technicians. Although I decided not to embark on a complete rewrite, we did redesign and rewrite those elements of the product (e.g. error handling and printing) which were very poor quality and responsible for the vast majority of the errors detected.

30. The decision was not as straightforward as some witnesses have proclaimed and was made solely on a commercial cost and risk basis. Many factors were material, not least the fact that we did not have an approved design specification, and whichever route was taken, there was significant risk that Fujitsu would suffer serious financial/commercial losses. Ultimately, the acceptance process would be the judge. It was certainly not an issue which could be swept under the carpet, the nature of the problems we were facing meant that if they had not been corrected, they would have surfaced again during the acceptance process and caused the roll-out to be delayed. As far as I can recall, POCL didn't seem to be under any undue pressure to start roll and certainly would not have given the go ahead had there been any known unresolved defects.

31. The reason for the recommendation to reconsider a EPOSS rewrite in the CSR+ review was due to the number of PINICL's outstanding, but this can be very misleading. To reiterate, PINICL's are incidents not necessarily software defects and not necessarily related to the EPOSS application installed in the counter, and this was the component which included examples of poor coding. A PINICL could be caused by a user error, inaccurate or missing documentation, a misunderstanding as to how the

WITN04190200

system was designed to behave and if a defect was discovered it may not have been in the product where the incident arose. All the outstanding PINICL's with an EPOSS tag were analysed in detail, categorised and fixed. Some were found in the Riposte messaging software, the reference data, the migration processes, the archiving/back up procedures, the end of day processes, consistent time clock interactions and the post office interface mechanisms (e.g. TIP). It is important to understand that the EPOSS comprised of several components in addition to the code which resided on the counter PC/Till. All these elements had to interact faultlessly if the end-to-end process was to satisfy the business requirements. The point being that even if the EPOS code in the counter had been perfect, accounting errors could still occur due to faults in the interfaces and interactions with other modules in the system. The only way to isolate the route cause would be to carry out a detailed analysis of all the known errors, which we did many times.

32. Another factor taken into account was that the task force had occurred almost 18 months before acceptance was due to take place. In that period, EPOSS had become a completely different product and had since undergone more extensive testing. To suggest that the product wasnt subject to repeated cycles of unit, link, system, integration, E2E and model office testing over several months is simply not true.

33. The decisions taken following the task force findings and the outcome from the review of CSR+ were made solely on a commercial cost and risk basis informed by the evidence available at the time see **[FUJ00079783]** & **[WITN04600104]**. They were transparent and legitimate as Mike Coombs

WITN04190200

was responsible for both development and support, so whatever the outcome, it would be Mr Coombs and Fujitsu who would suffer the consequences, and the option of a total rewrite of the software was still available should the circumstances dictate. The implications for POCL would be a delay of the roll-out and any political fallout that this would create. However, we genuinely felt that the business-as-usual software maintenance teams could handle the number of bugs likely to occur. There was no suggestion that people's livelihood, liberty or lives were being put at risk, and no ethical or morale implications to consider. Horizon was an administration and accounting system not an air traffic control or railway signalling system. The worse that could happen if important decisions subsequently proved to be ill-advised, would be additional cost for Fujitsu or a delay to the programme, or so we thought.

34. These decisions involved professional judgement, analysis of the evidence and an assessment of risk and feasibility and were not about supposition or speculation. The evidence given and claims made by David McDonald was his personal opinion, but equally there were others including myself, who felt that a complete rewrite was also fraught with risk. There were many factors influencing the decision such as, there could be integration/ interface issues which the documentation had not clearly defined, did we have sufficient skilled staff to take on the task, we did not have a detailed functional specification to refer to, there were massive regression testing implications and additional cost and timescale risks. Who's to say that had we chosen to totally rewrite the application that we

WITN04190200

wouldn't have incurred other problems which would have resulted in a similar or worse outcome?

35. Terms such as code decay, lack of robustness and shaky software have been banded around but how are these subjective terms quantified. Development history is only an indicator, a more relevant measure would be the number of category 1 defects found post live trial. The point I am trying make is that this is all about professional judgement, evidence and assessment of risk and not speculation. Post Office were aware of the known errors in EPOSS via the acceptance process and all the release notices and known error logs were circulated within the SSC and Help Desk community which included Post Office staff. It has been suggested that POCL should have been made aware of the development problems we had been experiencing so that they could request/demand more remedial work, but this argument could apply for declaring/explaining all the technical difficulties faced by ICL Pathway. This was never going to happen, firstly POCL were not in a position to contribute to a resolution, secondly as pointed out in paragraph 5 earlier, the PFI financial model was such that it was unrealistic to expect the supplier to allow the customer to influence/ degrade their business case and finally what purpose would it serve if the issues had subsequently been overcome. The comprehensive acceptance process was designed to provide customer with the ultimate assurance that the solution was fit for purpose. Does a car manufacturer tell its customers about the problems they encountered while designing and testing the steering geometry on their new model?

EPOSS & IT TERMINOLOGY

WITN04190200

36. The IT industry and the ICL Pathway team were guilty of using the same terms to mean different things. For example, *'performance'* can be used to describe how well a piece of software is doing its job, but it could also be referring to 'speed' such as the message response time at the counter, The term *'stability'* was often used to refer to the interaction between the Windows NT platform and the application, but it was also used to describe the overall reliability of a component. The former incidents would result in what was called a 'blue screen' event and/or 'system freezing' and were notoriously difficult to track down and required specialised technical expertise to identify the cause. The same applies to the term 'robustness' which can be used to describe any of the above events. This demonstrates that it is important to understand the context in which the term is being used, because issues can manifest themselves at the counter during an EPOSS session which are not necessarily caused by poor application code. A case in point were the email exchanges between myself and Steve Muchow referred to in my oral evidence, see **[FUJ00079333]**, which were discussing a 'performance/timing' issue with the end of day balancing process, not the performance/reliability of the product in general. It was possible that this problem was due to poorly written code, but it was more likely to be an issue with hardware capacity, system build, Windows NT or an interaction issue with other processes running on the Till at the same time.

EPOSS RELIABILITY

37. It was true that during the development phase EPOSS had been a cause for serious concern but by the time we entered the acceptance process we

WITN04190200

believed that the issues had been addressed or were in the process of being fixed. During the live trial every incident associated with cash accounting and/or balancing was subject to very close scrutiny to determine whether it was a software error, a mistake in the documentation, inadequate or insufficient training or an integration issue. I was in regular contact with Steve Warwick on the Help Desk who had been a senior member of the EPOSS development team, and I trusted his judgement due to his unrivalled knowledge of EPOSS and the post office accounting processes. This scrutiny continued into the roll-out phase, and we believed that the size and variety of the post office network was such that the large majority of undetected errors would surface relatively quickly. The development team wasn't aware that litigation and prosecutions were taking place during these early stages of roll-out.

END USER TRAINING

38. A unique aspect of the live implementation of the Horizon system was that it was not possible to carry out 'parallel running'. This is where the old manual system and the new computer system are run in parallel until it is proven that the results from the new system match the results from the old system. The reason why we couldn't do this was because the post office outlets did not have the human resources necessary to run two processes simultaneously. One of the major benefits from 'parallel running' was that it gives the end users time to learn the new system gradually.

39. ICL was responsible for developing the Training programme, but POCL was the overall approval authority and could veto any proposal put forward, even

WITN04190200

though the cost was being absorbed by ICL Pathway. I was responsible for training before Mike Coombs became Programme Director and implementing an effective training programme was considered to be a huge challenge right from the start. There were three reasons for this, firstly the sheer volume of people required to be trained (circa 40,000), secondly a large percentage of the post masters and mistresses were over 65, and at that time not familiar or comfortable with new technology, and finally the speed of roll-out specified by POCL (300 post offices per week) left little or no time for handholding or refresher sessions.

40. The training courses had to be of sufficient duration to cover all the subjects required but short enough to enable the students to spare the time. Many post masters/mistresses had to shut down the business while attending the course. It was also necessary to ensure that post masters/mistresses attended a course only a few weeks before their post office was due to be converted to the new system, otherwise the student could forget a lot of what had been learnt. If an installation was delayed, then the training would have to be rescheduled.

41. There was a lot of anxiety within the network and not surprisingly many post masters/mistresses were traumatised at the prospect of running their business manually one day and 24 hours later being fully automated. This represented a major risk to the success of the programme. Regional support staff who could visit branches who were struggling were an essential element of the overall training programme. Similar retail organisations such as supermarkets and banks do not have this huge problem to deal with.

WITN04190200

42. A training mode facility was developed to enable post masters/mistresses to try out the system and teach themselves how it worked without the fear of making mistakes and updating their data incorrectly.

43. All these issues put a much greater emphasis on providing a timely and knowledgeable 1st line support structure (i.e. Help Desk) operated by personal who were well versed in the post office end to end processes and the horizon functionality available on the till.

POST OFFICE WAS NOT AWARE OF BUGS, ERRORS OR DEFECTS

44. It has been stated many times during the Inquiry that staff in the Post Office were not aware of the bugs, errors or defects in the Horizon system at a particular time. This is strange because every release of the Horizon software was accompanied by a Release Notice and a Known Error Log. This would list all the functional changes which had been included in the release and identify all the known errors which had been fixed and as far as I know these were available to post office personnel.

45. All the errors and defects identified in the ICL Pathway solution, their severity and their status were documented at every stage of the testing and release processes

REMOTE ACCESS FACILITY

46. An approved specification for this functionality should be available to the Inquiry (CS/REQ/005). This type of capability was common practice and an essential part of a support technicians toolkit. Examples today would be products such as AnyDesk, TeamVeiwer and RemotePC, these enable someone to take control of another person's PC from a different remote

WITN04190200

location and are used by support organisations throughout the world. ICL Pathway also used a product called Tivoli to access all the remote counter tills to update software and associated data overnight.

47. It's not the facility that is the issue, it the effectiveness of the security processes which protected it and the completeness and accuracy of the record keeping. The ICL Pathway team were acutely aware of the risks involved in allowing access to a live system and implemented strict controls in accordance with the functional requirement specification. Access was only possible from specific PC's in specific secure locations, and was subject to restricted routing and used access tokens. My recollection was that following 'acceptance' and the start of roll out, the data in the post office branch was NOT accessible directly and was in fact encrypted. The only store which could be accessed was held on Servers in the Data Centres. The existing transaction data could not be changed, only new data added to resolve or neutralise a corruption or balancing issue which would later be resolved by a software change. I don't believe that it was mandatory to inform the postmaster/mistress that data had been added, but the operation was fully documented to show who had carried out the work, what they had done and when they did it. If a Post Office branch subsequently started to experience unexplained problems, the support team would be able to view the live access records to ascertain whether this action was responsible.

48. However, the fact that only the transaction data stored in the data centre could be accessed and not the data held in the branch PC/Till was purely semantics, because for recovery purposes the servers in the data centre

WITN04190200

and the counters constantly kept each other in sync. Therefore, whatever was present in the branch data held in the data centre would eventually be present in the branch PC and vice versa. This might explain why some of the claims in witness statements about what could and could not be done, appear contradictory.

USE OF THE TERM 'SYSTEMIC'

49. For what it's worth, I believe that most IT people would interpret the term 'systemic' to mean fundamental or system wide. For example, a design flaw in the way that errors were handled by all applications, or a problem with the way that all the interface mechanisms operated, or the consequence of the way that Oracle and Microsoft applications interacted. We would not consider an application error or defect to be a 'systemic' issue, but a process flaw impacting the way that all incidents were reported and resolved would fall under that definition.

SUMMARY

50. Most of the evidence given in Stage 2, included my own, explained, defended, or criticised decisions made which caused delays, resulted in extra cost or produced poor quality software. None of it explained why individuals subsequently lost their lives, liberty and livelihood. The general perception is that the software contained known and unknown faults when it shouldn't have done. However, this was an unrealistic expectation which could never have been satisfied and more importantly, was not the reason why postmasters/ mistress were treated the way they were.

WITN04190200

51. The reason for this appalling treatment was that the Post Office did not exercise healthy and sensible scepticism as to the maturity of the computer system to assist with fraud prosecutions and did not seek out corroborating evidence to support the case. It has been suggested that there had been a critical oversight by Fujitsu that the computer system was to be used to provide certified evidence for civil and criminal prosecutions. The Post Office may have been aware of this, but ICL Pathway were certainly not. If this requirement had been made clear during the early stages of the programme, it would have been a major topic for debate and potential disagreement. I do not believe that any organisation or individual can warrant the integrity and 100% accuracy of a computer system under any circumstances. Even if numerous checks and balances and sophisticated failsafe's had been built into the system and significantly more testing carried out, this risk would always exist. I would suggest that not only was there a breakdown in communication between the Post Office and Fujitsu but also between the Post Office legal dept and the Post Office IT dept. We have seen business requirements for PACE (certification) and the requirement to provide audit data (ARQ) but where is the business requirement to provide irrefutable evidence to support a prosecution case and to guarantee the accuracy and integrity of the data?

WITN04190200

I believe the content of this statement to be true.

Signed: GRO

Dated: 19/07/2024

WITN04190200

Index to Second Witness Statement of Terence Paul Austin

No.	Document Description	Control Number	URN
1	Letter from Keith Todd to Stuart Sweetman dated 10/03/1998 enclosing original letter to Peter Mathison dated 06/03/1998 and ICL Position Paper on the Pathway Project	POL-0027601	POL00031117
2	Handwritten note: Addressed to Dave [Millar] enclosing copy of Project Mentors Report of 18 December 1998	POL-0027615	POL00038829
3	Post Office Counters Ltd and ICL Pathway Limited Codified Agreement dated 28th July 1999	POINQ0006242F	FUJ00000071
4	Horizon Plan for Acceptance During the ICL Pathway Operational Trial (Version 2)	POL-0025619	POL00029137
5	CSR+ Corrective Action Plan (1)	POINQ0085954F	FUJ00079783
6	CSR+ Corrective Action Plan (2)	WITN04600104	WITN04600104
7	Email referring to EPOSS performance	POINQ0085504F	FUJ00079333