1. Claimants
2. Name of witness: Mr Richard Roll
3. No. of statement: 2nd
4. Date: 16 January 2019

THE POST OFFICE GROUP LITIGATION

Claim Numbers: HQ16X01238, HQ17X02637 & HQ17X04248

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION

BETWEEN:

ALAN BATES & OTHERS

Claimants

-and-

POST OFFICE LIMITED

Defendant

SECOND WITNESS STATEMENT OF RICHARD ROLL

I, Richard Roll, of **GRO** do say as follows:

1. I provide this statement for the purposes of the Horizon Issues trial listed for March 2019, and further to my first witness statement dated 11 July 2016.

2. As explained in my first statement, I was employed by Fujitsu between January 2001 and 2004. Prior to this, in 1976 I joined the Royal Air Force as an avionics engineer, I worked on a variety of mainframe computer systems and was selected for a software development team working on aircraft control and attack systems. Whilst in the RAF I attended night school and studied for an ONC in Electronics Engineering and an HNC in Software Engineering. After nearly 14 years, I left the RAF in 1989 and worked briefly in robotics before moving into a software development position in 1990. For the next 10 years or so, before starting at Fujitsu, I worked in a variety of development and support roles for international pharmaceutical and petrochemical companies (e.g. GSK, Eli Lilly, Shell). Since leaving Fujitsu, I no longer work in the industry. I left Fujitsu in 2004 to study full time at the University of Southampton and in 2007 I graduated with a BSc Honours degree in Podiatry. I practiced in the NHS until 2011 and since 2011 I have practiced privately in association with various Osteopathic and Chiropractic clinics. I currently have my own practice, "Wokingham Podiatry and Chiropody Clinic".

3. I have been asked to provide this statement to respond to some factual matters which are addressed in the expert report of Dr. Robert Worden dated 7 December 2018. In preparing this statement my attention has been drawn to particular paragraphs of Dr. Worden's report, within the sections headed *"4. Old Horizon (1998-2010)"* and *"11. Horizon issues - Facilities*

available to Post Office and Fujitsu", which I refer to below. I have not read Dr. Worden's report in full and do not attempt in this statement to provide a comprehensive response to it. The purpose of this statement is to address the discrete factual points which are within my knowledge and set out below.

4. The facts set out in this statement are within my own knowledge, or if they are outside my knowledge, I have explained the source of my information or belief.

Hardware Failures

5. Dr. Worden refers at paragraph 151 of his report to hardware failures. He says *"Although the hardware in the branches was not always reliable and communications infrastructure at that time were not highly reliable, there were strong measures built into Old Horizon to ensure that hardware failures and communication failures could not adversely affect branch accounts."* During my time at Fujitsu we frequently encountered hardware failures which had occurred in branches and required our intervention to attempt to remedy the problem. I would estimate that I was involved with a hardware failure on average at least once a month. These problems could and did affect branch accounts.

6. The most extreme case that I can recall was a complete failure of a counter to communicate with the server, which required the counter to be removed to the SSC so that the data could be recovered, and a replacement counter installed in the sub-post office. Prior to the problem being identified, data could be backing up on the counter without it being replicated to other counters or to the correspondence server.

7. I recall there were also PIN pad problems which caused issues in branches, and problems with other peripheral devices such as keyboards which only occurred intermittently, although I cannot recall the specific detail of these now.

8. I recall one particular case where branch data was not being replicated from a mobile post office correctly and it appeared that the subpostmistress was turning off the power mid transaction. As we could not fix this problem over the phone with the Subpostmistress, she sent the laptop to Fujitsu for examination. Using the Post Office test rigs on the sixth floor, and comparing the results with the laptop that had been returned to Fujitsu, I discovered that the button which should have put the laptop into standby mode was actually switching off the power, resulting in the disk crashing. I disassembled the laptops to confirm this. Thus, when the Postmistress thought she was switching her counter to standby mode, which would have initiated a controlled shutdown and allowed the datastore to replicate to the servers, she was actually switching the power off, which is what we were seeing in the SSC. When I raised this with my manager, Mik Peach, who subsequently talked to the hardware team, I found out that

this was a known problem: one of the engineers had made a mistake with a batch of laptops which had been sent out to branches before the error was detected. No-one outside the team responsible for building the laptops had been informed of this which meant that I had spent several days investigating the problem. Whereas the subpostmistress in this case was provided with a replacement laptop, knowledge of this problem was kept within the departments concerned and the batch of faulty laptops was not recalled. It is my belief that Fujitsu senior management and Post Office were not informed.

Transactional Integrity

9. At paragraph 156, Dr. Worden describes zero sum baskets, other branch actions being zero sum, and transactional integrity. I agree that the system was designed with these intentions in mind, but there were limitations and errors in the system. Data corruption and glitches sometimes meant that transactions were not zero sum. I recall on more than one occasion where subpostmasters had problems with a deficit showing in their accounts, and then as a result of working through a process to try to resolve it, the deficit doubled. Sometimes we found the source of the problem as a known bug (in the KEL) and we could resolve the problem, but we were not always able to find or understand the cause.

10. Some problems were very specific and arose rarely, hence we were not always able to predict these in advance. The following is a simplified example of one such problem which occurred on several occasions, I cannot remember the exact terminology so data types, company names and product types are for illustrative purposes only. Within Legacy Horizon, over 3,000 different products were offered for sale in post offices, with new products coming out and old products being withdrawn all the time. These products were identified by a 'business code' and 'product code'. Although some products were available in all Post Offices, other products were only available in a few post offices within a small geographical area and it is this type of product that caused the problem described below. A company called Local Electric Company (LEC) may have had a Business Code of 12345; and a bill payment to the LEC may have had a Product Code of 6789. If a customer paid an LEC electricity bill Horizon would concatenate these codes to create a unique product identifier, in this case 123456789. A new product, perhaps a salmon fishing license for the River Duffey (product code 56789) issued by North York Water (business code 1234), may have been added to the product list, so when a customer bought a salmon fishing license for the River Duffey the same Product ID (123456789) would be generated. At this point Horizon had no way of differentiating between these. The data would be replicated and the transactions harvested and processed overnight, and in this example all of the money would be transferred to North York Water and none to LEC. Fujitsu and the Post Office would be unaware of this until Subpostmasters started raising issues because LEC customers were complaining to them that their bills had not been paid.

Eventually the problem would be escalated to SSC and a work around established. Two points to note are that (1) the Business Codes and Product Codes were an industry standard which Fujitsu had no control over, and (2) when the software had been developed the developers were unaware of this potential problem; by the time it was discovered it was impossible to fix (the costs of redeveloping the system would have been astronomical).

11. I do recall that problems sometimes arose after subpostmasters used the recovery process and that this was a not uncommon problem which affected even experienced subpostmasters. This might suggest that there was a problem with the recovery process itself, or at least that it was not as straightforward as it should have been. However Fujitsu's stance was generally that if there was a problem with transactions following a recovery process and if SSC could not identify the cause, then the problem must have been caused by the Subpostmaster not following the recovery process properly. I recall that at the time I was not comfortable with this stance as there did appear to be wider issues here – just because SSC could not find a problem did not mean there wasn't one.

Transaction Corrections and Patterns of Software Errors

12. At paragraph 167 Dr. Worden describes software errors being corrected by Transaction Corrections, and states "*If there were any such software error, it would probably occur with such high frequency, and occur uniformly across all branches, giving rise to so many TCs, that Post Office would soon suspect a software error (for instance, seeing the effect repeatedly in some MIS report) and require Fujitsu to correct it.*" I do not recall Fujitsu carrying out any analysis of Transaction Corrections to try to identify if there may be an underlying software error. I also think it is wrong to say that software errors would occur uniformly across branches, as I explained in the example in para 10 above. My experience was that software errors occurred in very specific factual circumstances, which is why they were challenging to identify and correct.

13. Although it is correct that high frequency problems were found during testing, it was impossible to test for every permutation of data, and testing did not result in the identification of all errors.

14. I do not believe that it is realistic to say that all software errors would have been picked up by the processes which were in place, or that the likelihood of software errors staying disguised as human errors was very small (as Dr. Worden says at his paragraph 168). I believe there were likely many cases where subpostmasters would have been held responsible for problems which had not at the time been identified as software errors, either because they could not identify the problem and did not pursue these with Post Office or Fujitsu, or because when they were raised we (Fujitsu) were ultimately unable to identify the problem at the time. There

were, for example, bugs which created discrepancies such as transactions which subtracted rather than added values, and it was only with experience and investigation that we were able to identify these types of problem affecting a particular set of accounts. I do not believe that we were successful in identifying and correcting all problems. My experience of contacting subpostmasters is that they were generally very frustrated by the time we called them because they had been unable to find the source of the problem and had become quite cross about the perceived lack of support they had received (often by the time the SSC became involved, two or three days had passed).

Testing of software and development fixes

15. During my time at Fujitsu I know that there were budget pressures and redundancies which impacted system development and testing. The test team felt they were under enormous pressure to complete the testing within certain timescales which negatively affected the test regime. Meanwhile, the development team had to balance time spent on fixes, with time spent on developing new features for Legacy Horizon and time spent developing a new system which I believe later became Horizon Online

16. In my first statement, I refer to the pressure that the SSC team and Fujitsu were under generally due to an awareness of the financial penalties imposed by the Service Level Agreements between Post Office and Fujitsu (paragraph 12 of my first statement). I believe that although individual penalties were quite modest, when applied across multiple counters/post offices the cumulative figures involved were very high, potentially amounting to tens of millions or more. I disagree with Stephen Parker's statement that these potential financial penalties were not a factor for the SSC (paragraph 43 of Stephen Parker's witness statement) as we were aware of them and often commented on them, e.g. "That's saved Fujitsu another 25million".

17. A further limitation of the system and our support of it was that it was difficult to schedule fixes to be updated across the Estate. Updates were sent out to the Estate at night, but because it took several hours for the day's transactions to be replicated across to the servers, then there were new product releases and scheduled upgrades, and due to limitations in the bandwidth, it was not possible to send all updates out at the same time. In order to find adequate slots to send out updates, they had to be scheduled which contributed to the delay in getting them out.

18. Furthermore, when the developers released updates, there were occasions where previous work arounds used by the SSC for other issues not covered by the update no longer worked.

Identifying Unexpected Events

19. At paragraph 1087, Mr Worden states that *"Horizon's systems software generates events whenever something unexpected happens".* Whilst I agree that some "unexpected" events would be picked up by Horizon, there were many potential unexpected events that would not be picked up. Horizon's ability to identify unexpected events depended on how it was designed and programmed. For example, whilst the system may be programmed to recognise a figure that was nonsensically large, it may not be able to automatically identify an unexpected value of £1000 instead of £100. Generally this was a developing area, so generally if the SSC found something that should have been picked up by the system we notified the developers so they could fix the software, so it did incrementally improve over time. However, sometimes the decision was taken that the chances of the unexpected error happening again were too remote to merit a development/fix. In this case the developers would be instructed not to work on a fix.

Transaction Injection in Old Horizon

20. Dr. Worden refers at paragraph 1114 to the possibility of SSC injecting transactions in old Horizon, which is something I confirm that the SSC could do and that I did do this during my time at Fujitsu. However, Dr. Worden relies on the evidence of Mr Godeseth who says that any transaction injected by Fujitsu would be *"clearly distinguished"* by a counter position *"greater than 32"* because it would have been inserted at the correspondence server. However I think there is a very important factual point here, which is that whilst we could insert transactions using the correspondence server (and these would have a counter position greater than 32), we could also insert transactions remotely by using the correspondence server to piggy back through the gateway, to the individual counters in a branch. The nature of many problems meant that we had to implement a fix in this way rather than going to the correspondence server, and we frequently did use this method in practice. If we injected transactions in this way, at the counter position, then the counter position would be shown in the branch records and reports as the relevant counter position used in the branch (e.g. counter 1, or counter 2), and therefore not a number greater than 32 and not in a way which would distinguish it in any logs as having been inserted by Fujitsu rather than by the subpostmaster or an assistant. Sometimes we had to ask for a specific person to log in to the counter before injecting transactions so that the software would not detect any discrepancies. A transaction inserted in this way would appear to the subpostmaster as though it had been carried out through the counter in branch. I therefore disagree with Dr. Worden's conclusions that these transactions would always have been visible to subpostmasters (paragraph 1119), if he means to say that they would be shown to subpostmasters as transactions inserted by Fujitsu, rather than as transactions which appeared to have been created in branch.

21. At paragraph 1121, Dr. Worden states that *"as for transferring money, Horizon includes no functionality that allows payments to be made to external parties or account."* With reference to my first statement, which deals with this issue, I would like to clarify that whilst I was at Fujitsu, myself and the SSC team generally had the ability to inject data such that it had the effect to initiate the process to transfer money through the POL systems. Certainly when I started my role with Fujitsu, there was no limit to the type of transaction that we could insert. I do not have any knowledge or experience of this being done in practice, but the intention of my first statement was to identify this as a theoretical possibility due to the absence of controls on the ability for Fujitsu to modify branch data.

22. At paragraph 1144 Dr. Worden describes SSC's access to the counters as having been "strictly controlled". I do not think this was the case, as all SSC members had the ability to inject transactions as I have described above.

Rebuilding branch transaction data

23. As part of my role in the SSC, I was involved in rebuilding branch transaction data where a particular counter became corrupted. Whilst in general terms I agree with Dr. Worden's summary of this at paragraph 1131, his description is very much a simplification of the process, which was not straightforward. When data on a counter became corrupt, the effect was that data transmitted after that corruption could become stuck on the server for that counter and not be replicated to other counters, the gateway server or correspondence server. In order to correct the problem, we would have to copy the data after the corruption to our own computers, fix the corruption and then replace the data with our corrected copy and build this back on to the counter server. There was clearly room for error in this process, where data could be lost, or mistakes made when replicating data. As part of the rebuilding process, we were able to delete data from the counter server, and did this as part of the process I have described above. It was therefore possible that this process could result in data not being accurately copied across and/or data being permanently deleted. Data was occasionally lost because we were unable to copy it form the counter and thus were unable to rebuild the database correctly.

24. The process that I describe at paragraph 25 above could be carried out without the Subpostmaster's knowledge (which Dr. Worden acknowledges in principle at paragraph 1134) and in my recollection it sometimes was done without the Subpostmaster's prior knowledge, for example if the Subpostmaster was away from the branch on a lunch break and had not logged out of the system. Whilst in some circumstances we did notify the Subpostmaster in advance in order that they did not use the counter being worked on, there were times where the job needed to be done quickly to prevent potentially catastrophic failure and we were unable to contact the Subpostmaster beforehand.

Additional Clarifications

25. I have addressed this statement to responding to parts of Dr Worden's report as above, but I am aware that Mr Parker has provided a witness statement which responds to my first witness statement. I understand that permission for this witness statement is technically limited to me responding to Dr. Worden's report, and not a response to Mr Parker's statement. However if it is helpful to the Court for me to at least clarify my role, then I would add the following short points: (1) whilst my workload did involve some support to engineers opening and closing branches, I would estimate that this made up only 30% of my work, and the majority of my workload (estimate 70%) involved looking for faults on data stores, preparing reports for the manager as a result of reports of problems with Horizon experienced by the Estate, and (2) as part of this role, at least some of the time I was involved in examining source code; and (3) a group of perhaps 4 or 5 SSC staff could end up working on the same problem, but for recording purposes this would be assigned to one person (usually the person first allocated the task), therefore analysing the records where I am identified as the assigned person will not identify all problems which I worked on.

I believe the contents of this statement to be true.

Signed GRO R. Roll.

Date 16 Jan 2019