FUJ00179873

Filed on behalf of the: Defendant
Witness:
Statement No.: First
Date Made: 28 September 2018

Claim No: HQ16X01238, HQ17X02637 & HQ17X04248

THE POST OFFICE GROUP LIMITED
IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ROYAL COURTS OF JUSTICE

BETWEEN:

ALAN BATES & OTHERS

Claimant

AND

POST OFFICE LIMITED

Defendant

WITNESS STATEMENT OF TORSTEIN OLAV GODESETH

I, Torstein Olav Godeseth c/o Lovelace Road, Bracknell, Berkshire RG12 8SN WILL SAY as follows:

1. I am employed by Fujitsu Services Limited (**Fujitsu**) as Chief Architect on the Post Office Account.

2. I am authorised to make this statement on behalf of Post Office Limited (**Post Office**), the Defendant in these proceedings, in relation to the Horizon Issues trial listed for March 2019.

3. 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.

4. In this statement I refer to copy documents attached and marked Exhibit TOG1.

5. BACKGROUND

5.1 I graduated from Oxford University in 1974 with a degree in Natural Sciences (Physics). I worked for Rolls Royce (1971) Ltd from August 1974 until December 1976 as a Combustion Engineer. I joined the Royal Navy as an Instructor Officer in January 1977 on a Short Service Commission. In my final role in the Royal Navy I started my career in IT working in systems programming. I joined Forward Trust Ltd in November 1981 to work in systems programming and technical support for their IT systems. I joined the Post Office IT department in November 1987 to work on a project to introduce technology into Post Office branches. I worked with Post Office Counters Ltd as a technical advisor when they, together with the Benefits Agency, procured the Horizon system. I worked with Post Office Limited as a technical advisor when Banking was introduced. I was outsourced from the then Royal Mail IT department to Xansa in 2003 and was contracted to Post Office Counters Ltd to act as a technical advisor interfacing to Fujitsu and other suppliers providing IT services. I worked as an independent contractor to Post Office Ltd from 2005 till 2010 acting as a technical advisor on IT projects including the change of the Horizon system from Legacy Horizon to Horizon Online. I worked as an independent contractor for Fujitsu Services for 6 months in 2010. I joined Fujitsu Services as an employee in November 2010.

5.2 As Chief Architect I am responsible for ensuring that any changes made to the Horizon system are implemented without prejudicing the continued operation of the system. I work with architects and others in the technical community to agree the appropriate approach for making any changes.. A current organisation chart in relation to the Post Office Account is at pages [x] of TOG1As described below, Horizon is a large system and therefore it is not possible for one person to understand all corners of the system. I therefore have consulted with colleagues who work in the areas that are covered by this statement to ensure that my understanding of them is correct.

5.3 I understand from Post Office's solicitors that Post Office has given disclosure of technical documents about Horizon which describe the architecture of Horizon in detail, that the Claimants have only provided a high-level outline of their allegations against Horizon and that the Court has indicated that factual evidence for the Horizon Issues trial should be limited. Against this background, this statement provides a simplified overview of Horizon and addresses points that may (pending a full explanation of the Claimant's allegations) be relevant to the Horizon Issues to the extent that those points are not covered by the disclosed technical documents.

5.4 The following areas are covered in this statement:-

5.4.1 An overview of Horizon.

5.4.2 A description of the controls in place to ensure the accuracy of transaction data.

5.4.3 A description of Post Office's and/or Fujitsu's ability to remotely "access" transaction data recorded by Horizon.

5.4.4 Commentary on the Claimants' allegations that Post Office and/or Fujitsu remotely edited or deleted transaction data.

5.5 In this statement, I use the following defined terms:

5.5.1 "Horizon" means both Legacy Horizon and Horizon Online, as explained below and unless specified otherwise. [**DO WE NEED A MORE PRECISE DEFINITION OF HORIZON?**]

5.5.2 "Transaction data" means the record of transactions entered by branch staff on Horizon.

5.6 Where I say below that something is or is not possible within Horizon, I am describing my understanding of the functionality of the system as designed and implemented. It is of course possible that an error in the system or misuse by a system user could cause something unexpected to happen or for the system to be re-designed to do practically anything. This is the nature of all IT systems. Save where I expressly say so, I am not including these possibilities when commenting below. The development, testing and audit processes operated by Fujitsu to avoid errors in, or misuse of, the Horizon are described in the witness statement of my colleague, XXXX

6. HORIZON OVERVIEW

6.1 Horizon is the core operational and Electronic Point of Sales platform for the Post Office network. Fujitsu began work on a pilot of the system in 1996 and it was rolled out across the Post Office network between 1999 and 2002.

6.2 In 2010 there was a migration from the system commonly referred to as "Legacy Horizon" to an online version ("HNG-X" or "Horizon Online"). This was the biggest overhaul in the Horizon infrastructure that I can recall, although there have been continuous and ongoing iterative updates to the system over its life.

6.3 The key difference between Legacy Horizon and Horizon Online is the way in which data is stored. In Legacy Horizon, transaction data was stored locally on terminals in a branch and then replicated to the main data centres, usually several times a day. In Horizon Online, transaction data is recorded in real-time to the data centres[1]. This change was largely driven by the increased reliability and cost effectiveness of network connections during the period from 2000 to 2010.

6.4 Given that Horizon has constantly evolved and changed since its roll out in 1999, it would be a very arduous (perhaps even impossible) exercise to describe the

[1] HNG-X is being replaced by HNG-A. There is no functional difference between the two: HNG-A refers to an implementation of the same counter code as is used in HNG-X to run on a Windows 10 device (whereas HNG-X counters are NT4 devices).

system on every date it has been in operation. My comments below are about Legacy Online and Horizon Online in general and are accurate to the best of my recollection, recognising that this is a complex subject matter that has changed over an 18 year period.

6.5 Horizon's core requirement is to record the customer transactions and other accounting actions entered into by branch staff and then copy that information to Post Office and other organisations that need that information. The principal recipient is Post Office, but other recipients are, for example, Post Office's clients.

6.6 In simple terms, Horizon works as follows:

6.6.1 A user logs on to a counter in a branch using a unique user ID and password. The counter is much like any other personal computer with a keyboard for user input. The counter has a touchscreen and other peripherals such as a barcode scanner and a magnetic swipe reader. A PIN pad is connected to support banking and payment transactions

6.6.2 There are only, and have only ever been, four sources of transactions that make up transaction data:

(a) The vast majority of transactions are manually entered by a user in branch at the counter, by pressing icons on the touchscreen, keying in the transaction on the keyboard, scanning a barcode, scanning a magnetic card,or some other manual interaction with the system. These are referred to as "counter transactions".

(b) TCs are described in [**exhibit ARC/APP/ARC/0008**]. The process of generating a TC is largely a manual one run by Post Office. As I understand it, they are produced when Post Office compares the data entered into Horizon by branches with data generated from other sources in order to identify any discrepancies. TCs are sent to the branch via Horizon[2] from Post Office and then acknowledged by a user in branch. Before transaction corrections, a similar process existed called "Error Notices". These were sent to the branch in paper form and then manually entered into Horizon by a user in branch. Either way, it has always been a feature of Horizon that TCs and Error Notices required user input before they formed part of the branch's transaction records.

[2] TCs are incepted in Post Office's POLSAP system before being communicated to Horizon, via TPS to the BRDB.

(c) Third-party equipment located in a branch is required for some transactions, such as a Camelot terminal for lottery products and a Paystation terminal for some bill payments. These pieces of equipment communicate information direct to a client or other supplier, who relay that information to Post Office (or Fujitsu on Post Office's behalf), who then send a transaction acknowledgement (**TA**) to the branch via Horizon. A user in branch then needs to accept the TA on Horizon before it forms part of the branch's transaction data. TCs (formerly Error Notices) and TAs are known as "non-counter transactions" because the data does not directly originate from an interaction between Subpostmaster and customer at the counter in a branch.

(d) In Horizon Online it is possible for Fujitsu to insert a balancing transaction – see paragraph XX below. In Legacy Horizon it was possible to inject transactions into branch accounts - see paragraph XX below. In both cases such transactions would be clearly identifiable in the reports that can be obtained from Horizon in branches.

6.6.3 The transaction data is then communicated to the central data centres.

6.6.4 From there:

(a) One copy of the data is placed into secure storage, known as the Audit Store.

(b) Other copies (or parts thereof) are replicated to a variety of other systems, both inside and outside the Post Office's IT estate.

6.7 As can be seen from the above, all transaction data comes from, or is confirmed, by users in branch other than balancing transactions or their equivalent in Legacy Horizon. When transaction data is aggregated together, it is often referred to (in business speak) as the "branch accounts". In technical terms, the branch accounts are the product of a database query being run on the transaction data. For example, if a branch wishes to know how much cash it should be holding, Horizon adds up all the positive and negative cash movements shown in the transaction data and produces an aggregated number to the user.

6.8 Due to the different ways that Legacy Horizon and Horizon Online transfer and store data, I address them separately below when dealing with integrity of data being transferred through Horizon.

7. ACCURACY OF TRANSACTION DATA - HORIZON ONLINE

7.1 The master record of transactions entered in branch is often called "audit data".

7.2 The audit data collection and storage facilities within Horizon Online are described in the Audit Data Collection & Storage High Level Design document [**exhibit DES/APP/HLD/0030**]. As explained in that document:

> "*It is essential that the Audit System can both maintain the integrity of data under its management and subsequently be able to prove that integrity if and when the data is retrieved for analysis.*"

7.3 The core audit process is described in [**exhibit Fujitsu's core audit process presentation**]. This process is designed to ensure that transaction data inputted into Horizon in branch is communicated from the branch and stored in the Audit Store in a way that ensures the accuracy and completeness of that data.

7.4 When I use the phrase "accuracy" I mean that the data input in branch is faithfully replicated through the communication and storage process. I do not mean that the data accurately reflects the real transaction conducted over the counter between customer and branch staff. Put another way, if a member of branch staff inputs the wrong transaction on a Horizon terminal, the core audit process ensures that there is an accurate record of that inaccurate input. Save in limited circumstances, Horizon cannot know that the user has input incorrect data at the point when the transaction is undertaken.

7.5 A high level summary of the core audit process is as follows:

7.5.1 The transactions conducted on Horizon terminals in branches are bundled into virtual baskets (i.e. one basket of transactions per customer session).

7.5.2 Each basket is transferred over the network to the Branch Database (**BRDB**). The BRDB is hosted on a central server farm operated by Fujitsu (there is more than one BRDB server for resilience, and a set of gateway servers collectively termed the Branch Access Layer (**BAL**) are also used). The BRDB holds a live, but temporary, version of the transaction data used in day to day operations.

7.5.3 The basket is then transferred from the BRDB to the Audit Store via the Audit Server. The Audit Store is not involved in the live operation of a branch or Post Office's business; it is the long term repository of audit data.

7.6 I note that the above description focuses on transaction data but the Audit Store willalso contain some non-transaction information (e.g. log on to a terminal and moving cash in and out of a branch).

7.7 There are a number controls in place to protect the integrity of transaction data within Horizon (i.e. from the counter to the audit store):

7.7.1 In relation counter transactions:

(a) A basket must balance to zero, meaning that the value of payment taken / given by the branch from / to the customer equals the value of goods and services entered on Horizon. If the basket does not balance to zero, Horizon will reject the basket and it will not form part of the transaction data used to provide the branch's accounts ie. not part of the core audit process.[3] This control ensures that all transactions in the basket are recorded and also mitigates user error.

(b) A digital signature is calculated for the basket using a private key generated as part of the logon process and held at the counter. The counter also generates a public key which is returned to the BAL at logon so the BAL is able to confirm the source of all baskets it receives as coming from logged-on counters.

(c) Baskets must be atomically written, meaning that the whole basket is written to the BRDB or it completely fails to write the baskets. This is a control ensures that there can be no partial baskets.

(d) Each basket is given a unique Journal Sequence Number (**JSN**) of 1 greater than the previous basket so that the completeness (density) of the baskets from a particular counter in a branch can be checked. There is always a risk that when transmitting data over a network information may be lost. JSNs are the main control built into Horizon against this risk. If a basket were to go missing, there would then be a missing JSN. If a basket were to be sent twice, then there would be a duplicate JSN.[4]

(e) Baskets are signed by a digital signature, which in accordance with commonly adopted cryptography techniques, is used to secure the

[3] There will be a record kept of the rejected basket in other Horizon logs but it will not form part of the core audit process. CORRET?

[4] It should be noted that data other than baskets of transactions are communicated from terminal to the BRDB and so the JSNs do not necessarily run contiguously through all the baskets, but should be contiguous when all the audit data is reviewed.

integrity of transaction data once it has been initiated at the counter and allows the basket to be checked for subsequent interference once they have left the counter. This is a control against the risk of a basket being changed during transmission in such a way that it still "balances to zero" and has a contiguous JSN. In this scenario, the digital signature would be broken revealing that the content of the basket had been changed.

7.7.2 Non-counter transactions:

(a) TCs are presented to the branch for action ensuring that branch staff are aware of any impact on the branch accounts

(b) TAs must be accepted into the BRDB by branch staff by way of a TA in order to affect the branch accounts (branch staff can obtain reports from the Camelot, Paystation and formerly Post & Go terminals and compare those reports to the TAs that they are asked to accept to check that it is the same).

(c) Any processing of TCs or TAs are subject to JSN fingerprinting (i.e. the basket in which the TA or TC is accepted is subject to JSN fingerprinting) and signed by a digital signature.

7.8 All auditable messages (including transaction data and auditable event data) are written to a single table within the BRDB known as the “Message Log”. Each day the previous day’s Message Log is passed to the Audit Store[5] which then “seals” each file and stores them until they are retrieved (if they ever are) or deleted in line with the applicable retention period. This seal is cryptographically generated. Any subsequent change to the contents would invalidate the seal. The seal is held in a seals database separate from the audit data. A feature of the Audit Store is that data cannot be amended or deleted (even by Privileged Users) until the pre-defined “Purge Date”, which by default is set to 7 years. [**FJ - can Privileged Users amend or delete data in the Audit Store? Is the answer no, because they don't have the necessary permissions?**]

7.9 .

7.10 The Audit Store could be seen as the "master record" of the transaction data input in branch. It is designed to provide long-term, highly secure, storage of data in the event that any challenge to the data is raised. Save for it being a

[5] It is at this point that Horizon checks for missing or duplicate JSNs and reports any discrepancies.

repository of data, the Audit Store is not used in live daily operations by Subpostmasters or Post Office. A copy of the transaction data in the BRDB or in another system (see paragraph XX below) is used for day to day operations.

7.11 Post Office (its staff or it systems) does not have direct access to the Audit Store. Post Office may request data from the Audit Store via a process known as the "ARQ process" which requires manual intervention by Fujitsu staff to extract Audit Store data. The components that are used to provide audit data retrieval facilities are described in the Audit Data Retrieval High Level Design document [**exhibit DES/APP/HLD/0029**].

7.12 When audit data is extracted a number of completeness and integrity checks are carried out automatically as a matter of course including:

7.12.1 each entire audit file that contains data for the branch and period in question is checked to ensure that the digital seal described in paragraph **[insert cross reference**] is valid;

7.12.2 the data for the branch in question is then filtered out from these audit files and checks are then carried out on a counter by counter basis as described below for the period of the extract:

(a) a check to ensure that there are no missing or duplicate JSNs is carried out and the result of the check is recorded on the sheet labelled "Summary" in the standard ARQ report provided to Post Office;

(b) the Log on Message is checked and the digital signature generated by the BAL is checked by using the BAL's public key (which is known to the audit system), which shows that this message was signed by an application which had access to the BAL's private key. This then provides access to the counter's public key for that log on session (as this is included by the message audited by the BAL and was signed by the BAL's private key); and

(c) All subsequent messages sent from the counter to the BAL during that log on session are then checked to ensure that their digital signatures are correct (using the Counter's Public Key obtained from the Log On message).

7.12.3 The extracted data is then provided to Post Office, usually in the form of an excel spreadsheet as this is the most user-friendly format.

7.13 The number of ARQs issued since the 2014/15 financial year is as follows [**FJ - can we go back further than this?**] (1 ARQ = 1 month of an individual branch data, so one Post Office request for data could have multiple ARQs):[6]

7.13.1 FY 2014/15 = 729;

7.13.2 FY 2015/16 = 103;

7.13.3 FY 2016/17 = 323; and

7.13.4 FY 2017/18 = 364. [**FJ - does this figure need to be updated?**]

7.14 [**FJ - has the audit data been used to highlight faults in other data?**]

7.15 [**FJ - what (if any) additional checks are carried out/could be carried out by Post Office investigators?**]

7.16 As far as I am aware the above core audit process has always been used in Horizon Online. I am not aware of any bug, error or defect in Horizon Online that would cause the core audit process not to be effective.

8. AUDIT DATA - LEGACY HORIZON

8.1 Riposte was a messaging system which was responsible for storing all data in Post Office branches and replicating it to data centres

8.2 All counter data was held in a bespoke message store (which was part of the Riposte product supplied by Escher Inc.). This data was replicated within each branch to all counter positions and from each branch to the data centres where it was held in the correspondence server message stores. Similarly, any data inserted into the message store at the data centre (for example reference data or authorisations for banking transactions) would be replicated back to the branch counters.[7] Selected data was then extracted from the correspondence servers to update Post Office's back end systems.

[6] These figures do not include the ARQs that Fujitsu has issued in relation to these proceedings.

[7] Users with sufficient access permissions could inject additional messages at the correspondence server. Any additional messages injected at the correspondence server by users with sufficient access permissions included information including the identity of the user. That information would not be visible in the standard audit extracts, but it would be visible in a detailed examination of the raw audit data. Further, the node ID associated with the injected message would have been that of the correspondence server at which the message had been injected and not a normal counter node ID and that would have been clearly visible in any audit data.

8.3 All accounting at the counter was carried out based on the data held in the message store. The Riposte product managed the message store and it did not allow any message to be updated or deleted. Riposte allowed data to be archived once it had reached a sufficient age. Expiry varied by message type and also over time. It was never less than 34 days and by 2009 it was effectively 80+ days.

8.4 Each message included three key pieces of information which together provided a unique identification for each message:

8.4.1 Group ID: this was the 6 digit FAD Code of the branch with which the message was associated.

8.4.2 Node ID: this indicated the counter position at which the message was originally written for messages generated at the counter or the correspondence server identifier for messages generated at the data centre. Counter node IDs were between 1 and 31[8] and correspondence server node IDs were between 32 and 63.

8.4.3 Message ID: a unique number for each group ID / node ID. This number starts at 1 for the first message written at that node and increased by 1 for each subsequent message, which allowed checks to be made that no messages were missing as that would result in gaps in the sequence of message IDs (the concept of JSNs used in Horizon Online was based on this).

8.5 Messages also had an associated “Expiry Date” which denoted how many days after a message was first written that it could be deleted. An archive process ran on each counter and correspondence server at around 3am which deleted all messages that were past their Expiry Date, thus ensuring that the message store did not continue to grow indefinitely. .

8.6 Each message also had an associated "CRC", which was basically a checksum that was included to ensure that the message had not become accidently corrupted.

8.7 Due to the size of the Post Office Network, branches were split into four separate clusters and each cluster included four correspondence servers (two in each data centre), thus ensuring that there were therefore four copies of the data held in the data centres.

[8] Counter 31 indicated an exchangeable Hard Disk held in a single counter office as a back-up mechanism for the data as there was no other counter to replicate data to. No data should have been recorded as originating from node 31.

8.8 An audit application was run on the correspondence servers to take an audit copy of all data visible to that correspondence server. The audit application was run on one correspondence server on each cluster in each data centre. [The collected data, with the above controls in place, was then copied to the Audit Store CORRECT?]. This means that there were two independent audit trails for each branch. When retrieving the data only one audit trail was used.

8.9 The audit application read every record that was visible to that correspondence server (i.e. all data in that cluster) and wrote a text copy of that data to a text file. Each audit application wrote data to 10 text files (based on one of the digits in the FAD Code). When the text file got to a certain size it was closed and a new file created for that text stream. The file included a hash value of the file contents to ensure that should it be accidentally corrupted, then this would be detected. At around 1am each day the file was swapped to ensure that data associated with a given day was in discrete files.

8.10 Once these files had been written they became visible to the audit server which would pick them up, seal them and store them until they were retrieved or deleted in line with the applicable document retention period.

8.11 If the audit trail was retrieved, then similar checks to those carried out on Horizon Online were made automatically and in the normal course of business by the audit retrieval toolset namely:-

8.11.1 each entire audit file was checked to ensure that the digital seal stored at the time the audit was produced (i.e. the day after the transactions took place) was valid;

8.11.2 the data for the branch in question was then filtered out from the audit files and checks would then be carried out on a counter by counter basis for the period of the extract as follows:

(a) a check to ensure that there were no missing or duplicate message IDs for each counter / correspondence server would be carried out and the standard audit extracts into Excel included a report indicating that this check had been successfully carried out; and

(b) the CRC was recalculated and confirmed as correct for the message.

8.12 As far as I am aware the above core audit process has always been used in Legacy Horizon. I am not aware of any bug, error or defect in Legacy Horizon that would cause the core audit process not to be effective.

9. REMOTE ACCESS TO TRANSACTION DATA

9.1 I understand "access" to mean read only access to data stored in Horizon. I understand "remote" access to mean a user, using valid system credentials, directly accessing data stored in Horizon by means other than physically interacting with a terminal in branch.

9.2 As far as I am aware, Post Office employees could not access any transaction data stored in Legacy Horizon. Post Office employees with access to a system known as Horice can see some transaction data stored in Horizon. Horice provides a read-only near real time view on some data as it is captured in the BRDB.

9.3 Members of staff at Post Office can access copies of transaction data recorded by Horizon because that data is replicated to a variety of Post Office systems. I believe the main system that would be used by Post Office to view transaction data extracted from Horizon is Credence. Post Office can access summarised data received from Horizon in various SAP systems. I am aware that these SAP systems have changed in recent years and therefore the detailed interfaces from Horizon to Post Office 'Back Office' systems have changed and continue to change. **[FJ - is this how Post Office views transaction data? Can Post Office access/look at the BRDB? Or is it done via POL SAP or Credence? I think Credence or POL SAP and its successor(s)]**

9.4 **[FJ - in what ways can you view transaction data without being physically present in a branch? Credence or Horice]**

10. EDITING OR DELETING TRANSACTION DATA – POST OFFICE

10.1 Save as described in this statement, Post Office employees do not have the ability to insert or inject new transaction data into Horizon, or edit or delete transaction data stored in Horizon.

10.1.1 As explained in paragraph [x-ref], Post Office can / could send TCs, Error Notices and transaction acknowledgements to a branch via Horizon.

10.1.2 Post Office employees can visit a branch and log on to a terminal using Global User rights – described below.

10.2 The Claimants have asserted that Post Office and/or Fujitsu can insert, inject, edit or delete transaction data by way of:

""*global branches" (with branch codes such as 999998 and 999999), which would enable the input of transactions within Horizon as though it had come from an actual Branch*".[9]

10.3 Global branches are physical branches with Horizon terminals which are used solely for support purposes. Branch 999999 is located in Chesterfield and is used by Post Office. Branch 999998 is in Stevenage and is used by Fujitsu.

10.4 Global users are a category of users that can log on at any branch. Their username starts with an asterisk to differentiate them from other users. A number of employees of Post Office have, and as far as I am aware, have always had Global User accounts. I understand that Post Office uses these accounts to assist with certain branch operations such as opening / closing branches, training and audits. [**FJ - does FJ have Global User accounts?**]

10.5 There are a number of different types of global users as described in document ARC/SOL/ARC/0006 (a copy of which is at pages [x] of TOG1). [**Amy - has this doc been disclosed?**]. They are:-

10.5.1 MIGRATE - used to open new branches, setting the branch state from "New" to "Open";

10.5.2 AUDITOR - may view users and stock units etc. but not carry out transactions;

10.5.3 AUDITOR E - used by emergency managers to run branches;

10.5.4 ENGINEER - have the test capabilities that are required to perform branch maintenance and diagnostics;

10.5.5 SETUP - used for mobile / relief managers; and

10.5.6 SUPPORT - this is no longer used.

10.6 A global user can carry our transactions in the same way as an ordinary branch user as allowed by their allocated role. However, a Global User can only log on to a branch terminal and conduct transactions by being physically present in a branch. I would not consider this to be a form of "remote" access to (or remote injection, input, editing or deleting of) transaction data.

10.7 Transactions carried out by global users in branches will be shown in the branch transaction log (that can be accessed by branch staff) against the user ID

[9] Paragraph [**x**] of the Claimants' provisional / outline document in relation to the Horizon Issues dated 17 August 2018.

associated with the global user and therefore any transactions by a global user are distinguishable from other branch users.

10.8 When a Subpostmaster forgets their password, a user who is logged on at the Global Branch who has a role of ADMIN has the capability to reset their password. .

11. EDITING OR DELETING TRANSACTION DATA – FUJITSU

11.1 I address below the allegations raised by the Claimants about Fujitsu editing or deleting[10] transaction data. Save as described in this statement, I am not aware of any other way that Fujitsu could (theoretically) edit or delete transaction data. I should make clear that this is all largely hypothetical – other than the one occurrence of a balancing transaction (described below), I am not aware of Fujitsu ever having edited or deleted transaction data.

11.2 **Balancing Transactions (BTs)**

11.2.1 A small group of Fujitsu users from the Software Support Centre (**SSC**) (30 users) have the ability to inject additional transactions into a branch's accounts in Horizon Online, using a designed piece of functionality called a Balancing Transaction.

11.2.2 BTs are conducted using the branch transactional correction tool[11]. The tool is described in section 5.2.2 of the document [**exhibit DES/APP/HLD/0020**] and the Host BRDB Transaction Correction Tool Low Level Design document [**exhibit DEV/APP/LLD/0142**].

11.2.3 BTs do not require acceptance through the Horizon terminal by branch users unlike TCs and transaction acknowledgements.

11.2.4 BTs are clearly visible in the transaction reports that are available to Subpostmasters via Horizon as they are stated to have been carried out on counter number 99.[12] [13]

11.2.5 Audit data since 12 March 2010 [**Amy - has this been disclosed?**] shows that only one BT has been inserted into a branch's accounts.

[10] When I refer to deleting transaction data, I do not mean the final deletion of data once it has passed its set retention period.

[11] Note - this has nothing to do with TCs despite it being similarly named.

[12] Counter 99 would indicate that there were 99 serving positions in a branch, which no branch has, which is why this is readily identifiable.

[13] In legacy Horizon any transactions injected by SSC would have used the computer server address as the counter position which would be a number greater than 32, so it would be clear that a transaction had been infected un this way.

11.2.6 The TFS[14] helpdesk ticket relating to this BT (TFS ticket 2091569) [**Amy - has this been disclosed?**] was raised by Anthony Vasse of the Horizon Service Desk on 02 March 2010 and transferred to Cheryl Card (SSC Product Specialist). The ticket states that the clerk had incorrectly doubled a transfer of stock of £4,000 to £8,000, creating a shortfall of £4000 in the branch accounts. The issue required a resolution by 17 March 2010 because the branch was due to roll into the next trading period on that date.

11.2.7 The ticket was updated by Cheryl Card on 11 March 2010 to confirm that the issue had been resolved by inserting transactions into the BRDB_RX_REP_SESSION and BRDB_RX_EPOSS_TRANSACTIONS tables to reverse the incorrect £4000 charge. The ticket confirmed that the Subpostmaster had been advised to print a balance snapshot of the accounts before and after the BT took place to ensure the transaction had been reversed correctly. A subsequent update was provided confirming that the issue had been resolved and the ticket was closed on 04 April 2010.

11.2.8 The Peak Incident ticket raised in relation to the BT (PC0195561) was raised by Lorraine Elliot of the [Horizon] Service Desk [TBC] on 04 March 2010 [**exhibit**].

11.2.9 An OCP[15] ticket (25882) was also raised which is the solution management system used by Fujitsu which tracks issues and resolutions. [**Amy - has this been disclosed?**] This shows that the BT was approved by Emma Langfield of Post Office on 10 March 2010 at 15:33. The ticket was raised by Cheryl Card, who subsequently performed the work and inserted the balancing transaction.

11.2.10 A similar tool is used more routinely (although still infrequently) to update a flag which can become locked in the wrong binary setting (1, 0), preventing updates to stock units within a branch. This tool is described in [**exhibit DEV/APP/LLD/0202**].

11.3 Privileged Users

11.3.1 A limited number of authorised Fujitsu personnel (currently 19 at the operating system layer and 26 at the database layer) have access

[14] TFS is [the legacy system used by Post Office where branch incidents are recorded.] [**Need a better definition of TFS**]

[15] [**Insert description of OCP; predecessor of MSC**]

privileges that could be used edit or delete transaction data in the BRDB in Horizon Online (**Privileged Users**).[16] From the outset, I should make clear that this is only a theoretical possibility:

(a) Fujitsu has no policy, process, procedure or operational practice that calls for it to use its privileged access to edit or delete transaction data.

(b) As far as I am aware, Fujitsu has never used its privileged access to edit or delete transaction data.

11.3.2 [**FJ - what records do we have that show how many Privileged Users there have been historically? Awaiting confirmation from FJ (Matthew Lenton)**]

11.3.3 Privileged User access is required for system maintenance purposes, such as updating database records to implement change and planned system updates. Horizon has functionality to resolve the significant majority of imaginable operational errors in branch or technical errors in Horizon in the form of TCs and BTs. There is therefore little need to use privileged access to manipulate transaction data to resolve an error (BTs in particular are a deliberately engineered process to support the exceptional corrective processing). However, Privileged Users are still needed because there may be a need to make updates or changes to the core software that underpins Horizon. In my experience, the Privileged Users on Horizon have the same role as one would expect to see on any IT system. I would not consider them to be part of the functionality of Horizon but a fundamental building block that comes with any IT system built on databases.

11.3.4 [Hypothetical changes to a branch's transaction data in the BRDB by Privileged Users would be visible to branch staff. The amended transaction would show up in transaction reports that can be produced in branch, although it would not be flagged as a change by a Privileged User.]

11.3.5 [A key control in Horizon is the segregation of access permissions between Privileged Users who can access the BRDB and those users who may access the Key Management Server (**KMS**). The KMS holds the digital keys that underpin the controls regarding the integrity of data in Horizon. Segregation of Privileged Users from KMS users means

[16] There were no Privileged Users in Legacy Horizon.

that a Privileged User cannot get around these controls and therefore cannot cover up any changes they make in the BRDB.]

11.3.6 Since July 2015 all access and actions carried out by Privileged Users are recorded to an Oracle audit table. The audit table records information including:

(a) user ID;

(b) action; and

(c) date and time of the action; and

11.3.7 While a Privileged User could alter the audit table, the alteration of entries is recorded. This means that if an entry was removed, for example, the fact of the removal would be visible. If the audit table was removed, the database would stop working. All of these would be flag improper activity.

11.3.8 Prior to July 2015 the log on and log off activities by Privileged Users were audited. The process was for a Managed Service Change (**MSC**) document to be signed off and for the log on and log off records to be attached to the MSC. [**FJ - this means that we should provide the MSCs to the Claimants. To discuss**.]

11.4 The Transaction Information Processing Repair Tool

11.4.1 Fujitsu has provided information in relation to this tool in response to Jason Coyne's Request for Further Information 7.4 [**exhibit response to 7.4 only**].

11.4.2 The tool is described in the document that Fujitsu referred Mr Coyne to in response to RFI 7.4 (DES/APP/HLD/0020 Branch Database High Level Design) [**exhibit**]. It can only be used on data that has failed to be delivered between the Branch Database and the TPS system because it is missing a key attribute (i.e. one that is mandatory in the output files produced by TPS for Post Office back end systems) . This data is quarantined within the TPS system until the Transaction Repair tool corrects it. The correction is made on the TPS database and cannot directly affect the branch accounts in the Branch Database.

11.4.3 The tool was part of the TPS system which was moved, with limited functionality changes, from Legacy Horizon to Horizon Online and is still available in Horizon Online. In Legacy Horizon the tool could only be used on data that has failed to be delivered between Horizon locally and the TPS system.

11.5 [**FJ - are there any other ways that you can: (1) implement fixes in Horizon that had the potential to affect transaction data or data in branch accounts; or (2) rebuild branch transaction data?**] [**FJ - this still needs to be addressed**]

STATEMENT OF TRUTH

I believe that the facts stated in this witness statement are true.

Signed: ....

Date: ....