FUJ00159545

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

B E T W E E N:

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.

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 [**X**].

5. BACKGROUND

5.1 [**Torstein's education, work history and experience to be added**]

5.2 [**FJ - we need to explain Torstein's role as chief architect and the size/specialisms of the teams that he works with.**] As such, I 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 The following areas are covered in this statement:-

5.3.1 an overview of Horizon and the major changes since its introduction;

FUJ00159545

5.3.2 whether Post Office and/or Fujitsu are able to access transaction data recorded by Horizon remotely;

5.3.3 whether Post Office has the ability/facility to insert, inject, edit or delete transaction data or data in branch accounts;

5.3.4 whether Fujitsu has the ability/facility to: (1) insert, inject, edit or delete transaction data or data in branch accounts; (2) implement fixes in Horizon that had the potential to affect transaction data or data in branch accounts; or (3) rebuild branch transaction data;

5.3.5 how Horizon processes and/or records Transaction Corrections (**TCs**);

5.3.6 the core audit process in Horizon Online; and

5.3.7 the core audit process in Legacy Horizon.

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. In 2010 there was a migration from the system commonly referred to as "Legacy Horizon" to an online version ("HNG-X" or "Horizon Online"). The key difference between Legacy Horizon and Horizon Online is the way in which data is stored: locally in Legacy Horizon and centrally in Horizon Online. [**FJ - what is the main difference between HNG-X and HNG-A?**] There is no functional difference. 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). The mechanism for delivering the code to the counters is different for HNG-A.

6.2 [**Potted history of key dates and functional changes? Key dates from GJ's statement are: Network Banking 2003; Acceptance of Debit Cards 2003; EMV (ie use of Chip and PIN) 2004; Cash Account removed 2005; Data Centre Migration 2009; and HNG-X Rollout 2010.**]

7. WERE POST OFFICE AND/OR FUJITSU ABLE TO ACCESS TRANSACTION DATA RECORDED BY HORIZON REMOTELY?

7.1 [**FJ - are there any forms of remote access other than the ones dealt with in section 8 below that are used by Post Office to access transaction data remotely? (i.e. anything in addition to Balancing Transactions, Privileged**

FUJ00159545

Users and the Transaction Information Processing Repair Tool)? What transaction data does Post Office receive?]

8. DOES POST OFFICE HAVE THE ABILITY/FACILITY TO INSERT, INJECT, EDIT OR DELETE TRANSACTION DATA OR DATA IN BRANCH ACCOUNTS?

8.1 Post Office personnel do not have the ability/facility to insert, inject, edit or delete transaction data or data in branch accounts.

8.2 I understand that the Claimants' have asserted that Post Office and/or Fujitsu could do so 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*".[1]

8.3 The Claimants are referring to global users. Global users belong to either branch code 999998 or 999999 (they are managed through the [Post Office/Fujitsu] helpdesk which [is/used to be] split across two locations and there is a separate code for each location. [**FJ - please confirm which wording in square brackets is correct**]

8.4 Global users are auditors, engineers or emergency managers. [**FJ - are there any others?**] Auditors and engineers cannot conduct transactions. Emergency managers can conduct transactions when they are in branches. Such transactions carry the user ID 999998 or 999999 so it is clear that they have been conducted by a global user in the transaction and event data recorded by Horizon.

8.5 When a Subpostmaster forgets their password, a global user can cause a password reset. [**FJ - how is this done?**]

8.6 [**FJ - please provide the design doc that was referred to during the call on 28 August.**]

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

FUJ00159545

9. DOES FUJITSU HAVE THE ABILITY/FACILITY TO: (1) INSERT, INJECT, EDIT OR DELETE TRANSACTION DATA OR DATA IN BRANCH ACCOUNTS; (2) IMPLEMENT FIXES IN HORIZON THAT HAD THE POTENTIAL TO AFFECT TRANSACTION DATA OR DATA IN BRANCH ACCOUNTS; OR (3) REBUILD BRANCH TRANSACTION DATA?

9.1 The way in which transaction data is recorded by Horizon Online is set out in section [**x**] below. [At this stage it should be noted that branch accounts are stored in the Branch Database (**BRDB**) in Horizon Online whereas in Legacy Horizon the branch accounts were stored locally.] [**FJ - is it correct that the branch accounts are stored in the BRDB?**] The data is stored in BRDB so yes.

9.2 **Balancing Transactions (BTs)**

9.2.1 A small group of Fujitsu users (30 users) have the ability to inject additional transactions into a branch's accounts, through normal system functionality, via BTs. [**FJ - has this always been possible in Horizon? If not, when did it become possible? Are records available?**] The BT mechanism applies to HNG-X – not to Legacy Horizon

9.2.2 BTs are conducted using the branch transactional correction tool (this has nothing to do with TCs;[2] the tool was named before Post Office introduced TCs). 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**].

9.2.3 BTs do not require formal acceptance through the Horizon terminal by branch staff (unlike TCs and transaction acknowledgements).[3]

9.2.4 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/ [**FJ - has this always been the case? If not, when did the change/changes happen and what changed?**]

9.2.5 Audit data over the use of BTs is available from 12 March 2010 [**Amy - has this been disclosed?**]. Since that time, only one BT has been inserted into a branch's accounts. [**FJ - the audit data reviewed by Deloitte only went up to 28 May 2016 - please confirm that there have been no further BTs since that time.**]

[2] [**Insert description of TCs**]
[3] [**Insert description of TAs**]

FUJ00159545

9.2.6 The TFS[4] 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.

9.2.7 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.

9.2.8 The Peak Incident ticket raised in relation to the BT (PC0195561) was raised by Lorraine Elliot of the [Horizon] Service Desk [TBC] on 15 April 2010 [**exhibit**].

9.2.9 An OCP[5] 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.

9.2.10 [BTs are used more routinely (although still infrequently – 1,643 instances during the period of approximately 6 years) to update a flag which can become locked in the wrong binary setting (1, 0), preventing updates to stock units within a branch.]

9.3 **Privileged Users**

9.3.1 A limited number of authorised Fujitsu personnel (19 at the operating system layer and 26 at the database layer) have privileges to add / delete / change data in the BRDB (**Privileged Users**).

[4] TFS is [the legacy system used by Post Office where branch incidents are recorded.] [**Need a better definition of TFS**]
[5] [**Insert description of OCP; predecessor of MSC**]

FUJ00159545

9.3.2 [**FJ - what records do we have that show how many Privileged Users there have been historically? Awaiting confirmation from FJ**]

9.3.3 Privileged User access is required for system maintenance purposes, such as updating database records to implement change and planned system updates. [**FJ - does this explain why Privileged Users can alter transaction data?**] Horizon has functionality to resolve the significant majority of imaginable operational errors in branch or technical errors in Horizon in the form of transaction corrections and BTs. There is therefore little need to use privileged access to manipulate transaction data to resolve an error – such use would be a last resort and outside of mandated process (BTs in particular are a deliberately engineered process to support the exceptional corrective processing that less controlled privileged access would typically be used for). [**FJ - please provide an example of when it would be necessary to for a Privileged User to make a change rather than a BT**]

9.3.4 [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.]

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

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

(a) User ID;

(b) action;

(c) date and time of the action; and

(d) actual SQL statement executed (where applicable).

FUJ00159545

9.3.7 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.

9.3.8 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.**]

9.4 **The Transaction Information Processing Repair Tool**

9.4.1 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**]. [I confirm that this information is correct.] [**Andy - is this necessary?**]

9.4.2 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 key attributes [**FJ - what constitutes a key attribute?**].[6] 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 (or previously, Horizon).

9.5 [**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?**]

10. TRANSACTION CORRECTIONS

10.1 TCs are produced centrally by Post Office's Finance Service Centre (**FSC**). FSC compares the data entered into Horizon by branches [**FJ - what feed does Post Office use? BRDB? Audit Store?**] with data generated by other systems in order to identify any errors. One example of this is where Post Office compares the data entered into Horizon in relation to Bank of Ireland ATM's with data generated by the ATM itself.

[6] In Legacy Horizon the tool could only be used on data that has failed to be delivered between Horizon locally and the TPS system.

FUJ00159545

10.2 FSC inserts TC files into Horizon via the [**FJ - how is this done?**]

10.3 [**FJ - are there any documents which evidence these paragraphs?**]

11. AUDIT DATA - HORIZON ONLINE

11.1 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*."

11.2 The core audit process is described in [**exhibit Fujitsu's core audit process presentation**]. By way of a high level summary of the core audit process:-

11.2.1 Transactions conducted on Horizon terminals in branches are bundled into virtual baskets (i.e. one basket of transactions per customer) and securely transferred over the network to the 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).

11.2.2 Camelot, Paystation, and Post & Go transactions are conducted on their own separate terminals (hence they are often referred to as non-counter transactions) and accepted into the BRDB by way of Transaction Acknowledgments (**TAs**) on a daily basis.(Post and Go no longer supported – but that's detail)

11.2.3 The BRDB holds the live version of the transaction data used in day to day operations. Fujitsu also hosts other centralised data services to support reporting activities which are drawn from data on BRDB.

11.2.4 The audit records in the BRDB are transferred 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. [TG:

11.3 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):-

11.3.1 baskets of counter transactions:-

FUJ00159545

(a) a basket must balance to zero (e.g. the value of payment taken or given by the branch equals the value of goods and services provided);

(b) are atomically written (i.e. entirely or not at all) to the BRDB so that there can be no partial baskets; and

(c) are each given a unique Journal Sequence Number (**JSN**) of 1 greater than the previous transaction so that the completeness (density) of the flow of baskets from a particular branch counter can be checked when data is extracted from the audit store.

(d) are signed by a digital signature, which in accordance with commonly adopted cryptography techniques, is used to secure the integrity of transactional data once it has been initiated at the counter and allows all transactions to be checked for subsequent interference once they have left the counter.

11.3.2 non-counter transactions:-

(a) 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 Post & Go terminals and compare those reports to the TAs that they are asked to accept; and

(b) The only thing that is subject to JSN is the counter transaction/basket in which the clerk accepts the TA. The audit for the (external) transactions that the TA covers is outside of Fujitsu's domain. It's simply a record that the clerk 'accepted' a TA worth £x and the implication that if he was not happy then he would complain and resolve his concerns.

11.4 All auditable messages [(including transaction and event data)] [**FJ - is the wording in square brackets correct?**] [yes it's correct but not all events are auditable so there is scope for confusion – on balance happy though] are written to a single table within the BRDB known as the "Message Log". Each day the previous day's Message Log is written to a number of files which are then passed to the Audit system 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.

11.5 This seal is cryptographically generated and is based on the entire contents of the audit file. 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 System is that data cannot be amended or deleted until the pre-defined

FUJ00159545

"Purge Date". [**FJ - can Privileged Users not amend or delete it? If not, why not?**] There are software features that prevent purging before the 'Purge Date'. Note that we are currently holding data for longer than the standard 7 years but the 'Purge Date' protection only lasts for the 7 years. I think the 'Purge Date' is set at the time of writing the audit data to the audit system – will check the detail.

11.6 [JSNs, digital signatures and digital seals are applied by the counter's private key,][**FJ - is the wording in square brackets correct?**] [No – the private key is only relevant to the digital signature; JSNs are simple integers so the counter simply adds one. Digital seals are wholly inside the audit system and provide additional assurance that data has not been tampered with. The fundamental protection comes from JSNs and the digital signatures] which is generated by the counter as part of the log on process. A corresponding public key is included in the log on message that the counter sends to the BAL which allows the BAL to confirm that subsequent messages in the session come from the same counter (**Log on Message**). The BAL adds a wrapper to the Log on Message which includes a further digital signature (of the entire message including the counter's digital signature and public key) generated by the BAL, using the BAL's private key which is obtained from the NPS Key Store by the BAL at start-up.

11.7 Post Office Auditors may request audit data to assist with investigations in relation to branch accounts via a process known as the ARQ process.

11.8 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**].

11.9 When audit data is extracted a number of completeness and integrity checks are carried out [**FJ - are these checks done automatically as a matter of course?**],Yes including:

11.9.1 each entire audit file is checked to ensure that the digital seal described in paragraph [**insert cross reference**] is valid;

11.9.2 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;

FUJ00159545

(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).

11.10 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):[7]

11.10.1 FY 2014/15 = 729;

11.10.2 FY 2015/16 = 103;

11.10.3 FY 2016/17 = 323; and

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

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

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

12. AUDIT DATA - LEGACY HORIZON

12.1 Riposte is [**insert description**].

12.2 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. Selected data was then extracted from the correspondence servers to update Post Office's back end systems.

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

FUJ00159545

12.3 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.

12.4 Users with sufficient access permissions could inject additional messages at the correspondence server. [**FJ - why was this functionality present?**]

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

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

12.5.2 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 and correspondence server node IDs were between 32 and 63; and

12.5.3 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).

12.6 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.

12.7 Riposte was configured such that no messages where allowed to expire until they were at least 34 days old. This was to allow for counters that were offline for a significant period.

12.8 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. This was not a cryptographically secure seal.

12.9 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

FUJ00159545

centre), thus ensuring that there were therefore four copies of the data held in the data centres.

12.10 An audit application was run on the correspondence servers to take an audit copy of all data visible to that correspondence server.

12.11 The audit application was run on one correspondence server on each cluster in each data centre. This means that there were two independent audit trails for each branch. When retrieving the data only one audit trail was used.

12.12 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.

12.13 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. This process was not changed for Horizon Online.

12.14 If the audit trail was retrieved, then similar checks to those carried out on Horizon Online were made [**FJ - automatically and in the normal course of business?**], namely:-

12.14.1 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;

12.14.2 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.

FUJ00159545

12.15 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 [**FJ - who would have examined the raw audit data? Was it examined regularly?**]. 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 extract.

STATEMENT OF TRUTH

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

Signed: .....

Date: .....