POL00000686

Filed on behalf of the: Defendant
Witness: T. Godeseth
Statement No.: Third
Date Made: 28 February 2019

Claim No: HQ16X01238, HQ17X02637 & HQ17X04248

THE POST OFFICE GROUP LITIGATION
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

THIRD WITNESS STATEMENT OF TORSTEIN OLAV GODESETH

I, **TORSTEIN OLAV GODESETH** of Lovelace Road, Bracknell, Berkshire RG12 8SN **WILL SAY** as follows:

1. This is my third witness statement in relation to these proceedings. 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.

REMOTE ACCESS

2. In Mr Coyne's Supplemental Report (**Coyne 2**) he now places greater emphasis on "remote access". I covered this area in my first witness statement, but I have been asked to expand on my evidence below to address some points made in Coyne 2.

3. As explained in paragraph 47 of my first statement, 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. In the context of this litigation (which I understand to be primarily about shortfalls that have occurred in branches), I am focused on changes to transaction data as opposed to changes made to data in background operational parts of Horizon. By transaction data, I mean a record of a transaction undertaken in a branch with a customer or a branch activity that causes a change in the branch's cash or stock

{E2/1/13}

POL00000686

position (e.g. a remittance of cash); and I also mean the copy of that data that is used to generate the branch accounts for a Subpostmaster. Transaction data is copied to other systems that do not affect the branch accounts – those further copies and the systems on which they reside are outside the scope of this statement.

GLOBAL BRANCHES

4. Mr Coyne states that he has "...*formed the view that transaction capabilities were possible from the global branches situated within Fujitsu's work space...*" (paragraph 4.16 of Coyne 2). Mr Coyne refers to two documents in support of this view: Peak PC0205725 {POL-0375491} and design document DES/GEN/SPE/0007_6.2 {POL-0153568}. {D2/4/99}

5. In paragraph 54 of my first statement I set out the different types of global users listed in document ARC/SOL/ARC/0006 {POL-0440076}. The quote that Mr Coyne has taken from Peak PC0205725 in Coyne 2 simply describes what types of global user can log on where. It does not state that global users can conduct transactions remotely. {E2/1/15}

6. The table to which Mr Coyne refers from design document DES/GEN/SPE/0007_6.2 {POL-0153568} contains both local users and global users. The "Clerk" role to which Mr Coyne refers in paragraph 4.19 of Coyne 2 is a local user: this is clearly stated in the ARC/SOL/ARC/0006 document {POL-0440076} that I referred to in my first statement. A local user is a user that is set up for a specific branch and can only log on in that branch. {D2/4/100}

7. In my second statement I stated in paragraph 31 that Branch Code 999993, a Global branch in Wakefield was closed in September 2016. The record for this branch in the Branch Database (**BRDB**) shows that it was opened in early 2013. I understand that it was used to provide out of hours cover. It was closed when Fujitsu Services were no longer required to provide this service. {E2/7/9}

8. In paragraph 51 of my first statement I explained that transaction data or other data in branch accounts cannot be inserted, injected, edited or deleted by someone logged into a global branch but not physically present in a branch and my evidence remains unchanged having read Coyne 2. The technical explanation for this is that: {E2/1/14}

8.1 when a user logs on at a terminal in a branch (it matters not whether that is a global branch or an ordinary one), the user cannot specify the FAD code (i.e. the branch code) or the node they are logging on to – that is fixed by the terminal which has been set up to have a specific network address;

POL00000686

8.2 when the terminal sends messages to the BAL, the branch code and terminal ID are included in the messages and BAL checks the address that the message came from and confirms that these all match (i.e. that that network address corresponds to the branch code and terminal);

8.3 if the message received is auditable, as any message containing transaction data will be, it will be written to the Message table using the branch code and terminal ID as part of the key; and

8.4 digital signature checks on each message coming from the terminal will confirm that the message is part of a session being run from that specific terminal.

9. Whilst no global users have been set up with Clerk permissions, some global users do have permissions assigned which allow them to carry out transactions, and as part of their duties they will visit post offices, log on and carry out transactions. As explained above, they have to be physically present in the branch to do this. Any transactions carried out whilst they were logged on will be written to the BRDB for the branch and node for the physical terminal at which they are logged on: they would be clearly identifiable.

TRANSACTION INFORMATION PROCESSING (TIP) REPAIR TOOL

10. Paragraphs 3.234 to 3.248 of Coyne 2 refer, inter alia, to Peaks that relate to the use of the TIP Repair Tool and from which Mr Coyne draws conclusions that this is evidence of "balancing transactions" being added to branch accounts. That is not correct. First, these are not "balancing transactions" - see paragraph 24 below. Second, in paragraph 60 of my first statement I described the TIP Repair Tool and explained that this does not have an impact on branch accounts. My evidence remains unchanged having read the above parts of Coyne 2. I provide a further explanation below.

{D2/4/73}; {D2/4/74}; {D2/4/75}; {D2/4/76}

{E2/1/18}

11. The TIP Repair Tool (which was available in Legacy Horizon and is available in Horizon Online) is used on data that has failed validation on the transfer between the BRDB and the TPS system in Horizon Online and is therefore quarantined within TPS. I understand from speaking with colleagues that it served a similar role in Legacy Horizon in relation to data moving between the Riposte Message store and the TPS system. The TPS system is used to transfer data out of Horizon and on to other external systems. The TPS system (in either Horizon Online or Legacy Horizon) does not hold or generate data that is used to produce a branch's accounts from a Subpostmaster's perspective. Accordingly, an error or change in TPS data will not affect a branch's accounting position.

POL00000686

12. The TIP Repair Tool is used where the format or content of the data output from Horizon is incompatible with the systems to which it is being delivered. For example, a system may require that certain data fields are populated. If these criteria are not met, the receiving system may reject the data. The TIP Repair Tool is used to correct these incorrect or missing attributes. The correction does not change the core information about the transaction. For example, PC0159759 {POL-0330030} shows mandatory fields (Startdate, StartTimeFraction, EndDate and EndTimeFraction) were omitted from four messages and the TIP Repair Tool was used to insert suitable values. These are all timestamps so have no impact on accounts, but the receiving system expects the fields to be there. In practice, there are multiple timestamps in messages, so other, appropriate timestamps would have been used (which may differ by a few seconds from the missing one).

13. The changes are made to the data in the TPS system not in the BRDB (or the Riposte Message store in Legacy Horizon).

REMOTE ACCESS IN LEGACY HORIZON AND HORIZON ONLINE

14. Having further explained that global users and the TIP Repair tool cannot insert, inject, edit or delete transaction data remotely, to the best of my knowledge, the following types of remote access, as defined in paragraph 3 above, are or have been possible:

14.1 Privileged users could, theoretically, inject, edit or delete transaction data in Legacy Horizon (as noted in paragraph 37 of my first statement, the Riposte product that managed the message store and it did not allow any message to be updated or deleted, but theoretically a user with sufficient access rights could do so elsewhere in the system). As far as I am aware, this never happened. {E2/1/11}

14.2 Members of the SSC could inject transaction data into a branch's accounts in Legacy Horizon.

14.3 Privileged users can, theoretically, inject, edit or delete transaction data in Horizon Online. As far as I am aware, this has never happened.

14.4 Members of the SSC can inject additional transactions into a branch's accounts in Horizon Online using a designed piece of functionality called a Balancing Transaction (**BT**). Audit records show that this has happened once.

14.5 In Legacy Horizon, Fujitsu could cause data to be rebuilt from copies of the same data as described in paragraphs 36 to 38 of my colleague Steve Parker's second witness statement.

POL00000686

15. Coyne 2 contains a number of misunderstandings in relation to these types of "remote access" and I will clarify the position below.

PRIVILEGED USER ACCESS

16. In paragraph 59.1 of my first statement I explained that there are small number of users who have access privileges that could (in theory) be used to edit or delete data in Horizon (to be clear, with enough access rights a privileged user could theoretically inject data, too). Mr Coyne concludes in paragraph 5.449 that privileged user access is in fact being used to edit or delete transaction data in the BRDB. He does not expressly cite the parts of his analysis in Section 3 of Coyne 2 on which he relies to reach this conclusion. His conclusion expressly refers to the BRDB which is a database that only existed in Horizon Online, so I presume that his conclusion is limited to Horizon Online. Post Office's solicitors have drawn my attention to the following potentially relevant parts of Coyne 2 that could relate to this subject matter in the context of Horizon Online: {E2/1/17}

16.1 three situations where Mr Coyne believes that Fujitsu is deleting transaction data from Horizon Online at paragraphs 3.266, 3.270 and 3.271; {D2/4/80}; {D2/4/81}

16.2 paragraph 3.277 where he refers to the APPSUP role; and {D2/4/82}

16.3 paragraphs 3.281 and 3.316 which set our Mr Coyne's review of the Privileged User access logs. {D2/4/83}; {D2/4/91}

17. In paragraphs 3.266 and 3.271, the references to deleting session data are describing where Fujitsu is deleting or changing data in a database table in the BRDB that does not hold transaction data. On rare occasions, this is needed where a marker is recording a situation that is out of sync with the position in the branch. For example, as part of the normal rollover process a user will lock a stock unit resulting in a flag in the BRDB being set to 'Y'. The effect of this flag is to constrain other users who may be using the same stock unit. This may be untenable in the branch – if for example the user who locked the stock unit is not available to unlock it. Fujitsu may be requested to amend that database entry to allow the branch to carry on using the stock unit. To be clear, no transaction data is being affected and so this type of change cannot be the cause of shortfalls or surpluses in branch accounts. This might seem like a fine distinction, but it is a critical one. Whilst deleting operational data from specific tables in the BRDB must be done with care it is the appropriate way to handle some problems in order to keep the system running. Deleting transaction data is a very different thing. {D2/4/80}; {D2/4/81}

POL00000686

18. The Peak referred to in paragraph 3.270 does not record the deletion of transaction or any data at all. This is clear from the Peak itself which Mr Coyne appears to have misread. {D2/4/81}

19. Paragraph 3.277 describes the APPSUP role and refers to a Peak in which there is a general discussion on the level of permissions required by SSC staff to fulfil their role. APPSUP is the more technically accurate name for a role with Privileged User access to the BRDB and other parts of the system. Although the APPSUP role could theoretically be used to inject, edit or delete transaction data, this Peak does not provide any evidence of this actually happening. It is discussing the administration of the APPSUP role rather than its use in a particular situation to change live transaction data. {D2/4/82}

20. At paragraphs 3.281 and 3.316, Mr Coyne states that the has reviewed the Privileged User logs that have been disclosed as part of these proceedings which show the number of accesses to Horizon Online by different Privileged Users. While I have not had the opportunity to review and analyse those logs, it should be noted that system access does not mean that transaction data was changed and, as noted above, as far as I am aware this has never happened. {D2/4/83}; {D2/4/91}

21. Having read the above paragraphs of Coyne 2 and the associated Peaks, none of them show transaction data being edited or deleted. I am still not aware of any example of such access being used to edit or delete transaction data in Horizon Online (or to inject transaction data).

22. Mr Coyne also says at paragraph 5.427 that there is a risk that privileged users could make mistakes when working in the BRDB that could lead to mistaken changes to transaction data. As stated above, I am not aware of any example of such access being used to edit or delete transaction data in Horizon Online, but even if they did I think the risk of mistakes being made would be extremely low. Fujitsu builds tools to avoid having to do things manually and when we do have to do things manually we have policies of involving at least two people when working in the databases to minimise the risk of user error. {D2/4/242}

23. Even if someone were minded to manually make a change to transaction data in the BRDB or did so accidentally, the chance of any significant change being done without it being detected is vanishingly small. Transaction data is recorded in the Message table where it is protected by digital signature and the data held in this table and subsequently the Audit store is the ultimate reference copy of the transaction data. Making changes to copies of the transaction data in other tables in the BRDB would be visible to the Post Office branches carrying out balancing

POL00000686

against cash and stock in the physical branches and would trigger off an investigation.

BALANCING TRANSACTIONS (HORIZON ONLINE)

24. Mr Coyne appears to use the term "balancing transaction" to mean any change to Horizon data (not just transaction data) by Fujitsu using any of the above methods in any version of Horizon (see paragraph 5.488 of Coyne 2). This is not a correct use of the term given that, as I explained in my first statement, a BT is the result of a specific designed piece of functionality in Horizon Online only. A "balancing transaction" is a BT conducted using the Transactional Correction Tool. It is inaccurate to use it in the general sense used by Mr Coyne. Based on this correct definition, I stand by paragraph 58.5 of my first statement – that as far as I am aware there has only been one BT used to insert transaction data. {D2/4/259} {E2/1/16}

INJECTING TRANSACTIONS (LEGACY HORIZON)

25. In paragraph 58.10 of my first statement I stated that any transactions injected by SSC in Legacy Horizon would have used the computer server address as the counter position which would be a number greater than 32. I have read Parker 2 and I am now aware that it was also possible for SSC to insert transactions with a counter position with a number less than 32. I did not discuss this in my first statement because I was not aware of it. {E2/1/17}

STATEMENT OF TRUTH

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

Signed: GRO

Name: IORSTEIN GODESETH

Date: 28th Feb 2019.