POL00029104

Confidential and subject to litigation privilege

Bond Dickinson

SUMMARY OF DELOITTE'S BRAMBLE REPORT DATED [31 OCTOBER 2016]

1. INTRODUCTION

1.1 Allegations have been made by Claimants that Horizon does not accurately record the transactions input by postmasters. Further, it is alleged that Post Office / Fujitsu has the ability to add / delete / change transactions recorded by branches without the consent / knowledge of a postmaster.

1.2 To address these allegations Deloitte has undertaken a review of certain aspects of Horizon. They have a produced a full report on their findings.

1.3 This document is a summary of Deloitte's investigative work. It is designed to be easy to read and therefore necessarily simplifies the complexity of the Horizon system and the nuances of Deloitte's analysis. It does not cover all of the findings, assumptions and limitations noted in Deloitte's report.

2. EXECUTIVE SUMMARY

2.1 All transactions recorded by Horizon that make up the branch accounts are either input or approved by Branch staff before they form part of the branch accounts save for:

2.1.1 transactions input by POL and FJ staff setup as Global Users (see section 7 below);

2.1.2 Balancing Transactions (section 5 below); and

2.1.3 amendments to databases that underpin Horizon made by Super-users (see section 6 below).

2.2 Once a transaction is input or approved by a branch, there are a number of controls in place to protect the integrity of that transaction data and Deloitte has confirmed that these controls are generally effective save in a few respects, at least one of which is already known to be a material concern (see below regarding super-users) and certain others that are under further review (see section 4 below).

2.3 There are a number of authorised staff at Fujitsu who have "super-user access" to the databases that form the Horizon system. This access theoretically allows those staff to add or delete transactions or make changes to transactions recorded by branches. Depending on how the amendments are made and in which databases the amendments are made, these amendments could change a branch's accounting position in the real world (e.g. it could create a fictitious loss).

2.4 Horizon is designed in such a way that super-user activity is either automatically logged or would leave behind a footprint showing that changes were made to transaction data. To ensure that this log / footprint cannot be wiped away, super-users should not have access to these controls with the controls being operated by a separate group of users (the so called Segregation of Duties).

2.5 Deloitte have determined that certain super-users also have sufficient access rights to circumvent some of these controls. These users could theoretically (albeit with great effort and in limited circumstances) make amendments to Horizon transaction data and then cover their tracks so that no log / footprint of the changes would be left behind. The Segregation of Duties was a known part of Fujitsu's control framework and Fujitsu appears, anecdotally, to have accepted that the failure to implement this control was an oversight on its part.

3. SCOPE OF DELOITTE'S WORK

3.1 Deloitte was instructed to carry out work in relation to three scope areas:-

POL00029104

3.1.1 An analysis of data in respect of 13,307,999 transactions and data in respect of 5,289,369 events relating to branches within the mediation Scheme to confirm, insofar as possible, whether any bugs in the Horizon system are revealed by the dataset which caused discrepancies in the accounting position for any of those branches.

3.1.2 A full review of the use of Balancing Transactions throughout the lifetime of the Horizon system, insofar as possible, to independently confirm from Horizon system records the number and circumstance of their use; and

3.1.3 A full review of the controls over the use and capability of authorised Fujitsu personnel to create, amend or delete baskets within a sealed audit store throughout the lifetime of the Horizon system, insofar as possible.

3.2 After initial work was carried out, further clarification questions were added to the scope of work (for example, Deloitte were asked to look at the ability of Fujitsu to amend data in other databases outside the Audit Store).

3.3 In broad terms, Deloitte investigated these questions through four routes:

3.3.1 By reviewing Horizon technical documentation provided by Fujitsu.

3.3.2 By asking questions of key Fujitsu staff.

3.3.3 By reviewing transaction and event data generated by Horizon.

3.3.4 By walking through some of the Horizon processes on screen with Fujitsu.

3.4 No analysis was undertaken on Horizon's source code.

4. DISCREPANCIES IN RECORDED TRANSACTIONS (SCOPE AREA 1)

4.1 A diagram showing the high level flow of data from transaction origination through to the Audit Store is set out in the Appendix to this document. In summary:-

4.1.1 Transactions conducted on Horizon terminals in branches are bundled into virtual baskets (i.e. one basket of transactions per customer) and transferred over the internet to the Branch Database. The Branch Database is a central server operated by Fujitsu.

4.1.2 Non-Counter transactions (such as Paystation) must be accepted by branch staff on a Horizon terminal in a branch by way of a Transaction Acknowledgement before they are then recorded in the Branch Database.

4.1.3 The Branch Database holds the live version of the transaction data used in day to day operations. For example, when a postmaster in a branch requests on his local Horizon terminal a list of all the transactions conducted on a specific day, this data is drawn from the Branch Database and sent over the internet to the terminal in the branch.

4.1.4 From the Branch Database, transaction data is fed into various other Post Office systems that then connect to various third party systems.

4.1.5 The transaction records in the Branch Data are also 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 transaction data. In the event of a challenge to the integrity of any transaction data, the Audit Store is considered to be the master record.

4.2 There are a number controls are in place to protect the integrity of transaction data within Horizon (i.e. from branch terminal to Audit Store).

4.2.1 Counter transactions:-

POL00029104

(a) 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 Branch Database so that there can be no partial transactions; and

(c) are each given a unique Journal Sequence Number (**JSN**) of 1 greater than the previous transaction ("digitally signed") so that the completeness (density) of the flow of transactions from a particular branch can be checked when data is extracted from the Audit Store.

4.2.2 non-Counter transactions:-

(a) must be accepted by branch staff by way of a Transaction Acknowledgement in order to affect the branch accounts; and

(b) contain interface files which are used by Horizon to check the completeness of data [Deloitte – does this mean that Horizon checks that non-Counter transactions balance to zero?] and which can be used to verify data integrity when data is extracted from the Audit Store.

4.3 There are also recovery processes that operate in the event of connectivity issues (when a branch terminal cannot connect to the Branch Database).

4.4 Deloitte reviewed the Transaction Logs and the Events Logs and made two observations which may show that the above controls are not fully effective:-

4.4.1 There were 212,372 gaps in the Journal Sequence Numbers from a total of 13,307,999 transactions which means that there are 212,372 missing baskets. All of these gaps post-dated the introduction of Horizon Online. This could be indicative of connectivity issues (which is a known issue and not a material concern) or something else.

4.4.2 There were 59 baskets, all pre-dating the introduction of Horizon Online, from a total of 3,074,830 that did not balance to zero. In accordance with the controls above, all baskets should balance to zero.

4.5 At this stage it is not known whether the above issues are material or not. Consideration is being given to what further enquiries should be taken to investigate these issues further.

5. BALANCING TRANSACTIONS (SCOPE AREA 2)

5.1 Balancing Transactions are exceptional processes used by Fujitsu support staff to correct exceptional errors in system processing/fix issues or bugs in the recording of data in Horizon Online. (It is not known whether Balancing Transactions or an equivalent existed in Legacy Horizon and answering that question is now difficult due to the passage of time). Given that controls are in place to prevent such issues, the incidence of Balancing Transactions should be inherently low.

5.1 Balancing Transactions are the only transactions that do not either originate in the branch or have to be acknowledged / accepted in branch. A single Balancing Transaction can insert a single additional transaction of either positive or negative value into a branch's accounts. They can, if misused, have the effect of creating a fictitious loss or gain.

5.2 The following key controls are in place to regulate the use of Balancing Transactions in Horizon Online:-

5.2.1 Balancing Transactions can only be performed by a limited number of authorised Fujitsu personnel (31 users).

POL00029104

5.2.2 If a Balancing Transaction is used a record of it is created in the Audit Store (this is known as an audit file).

5.2.3 Fujitsu staff who are authorised to post Balancing Transactions cannot amend the related audit files.

5.3 Balancing Transactions are identifiable in branch. They appear on the Transaction Log report that can be produced by branch staff. They are shows as transaction against the user ID "SUPPORTTOOLUSER99" rather than the user ID of any member of staff at the branch.

5.4 Deloitte reviewed audit data over the use of Balancing Transaction for the period 12 March 2010 to 28 May 2016. Earlier data was not available. Deloitte found that a Balancing Transaction was only used once to change a branch's accounts over the period. This was a known and approved use of a Balancing Transaction in special circumstances. It did not affect any Claimant.

5.5 Other uses of Balancing Transactions over the period reviewed did not involve changes to transaction data and could not therefore have affected a branch's accounts.

5.6 The above findings in relation to Balancing Transactions are subject to the findings below in relation to super-users. In theory, super-user access could be used to circumvent the above controls.

6. SUPER-USERS (SCOPE AREA 3)

6.1 There are a limited number of authorised Fujitsu "super-users" (26) [Deloitte – please confirm that this number is accurate] who have sufficient privileges to theoretically edit and/or delete transactions in the Branch Database. It is not uncommon for there to be super-users in relation to systems such as Horizon.

6.2 As branch accounts draw on data from the Branch Database, edits or deletions in the Branch Database could impact upon branch accounts.

6.3 The following key controls regulate super-user activity in Horizon Online:-

6.3.1 Counter transactions are "digitally signed" (i.e. they are given a unique JSN of 1 greater than the previous transaction) so that the completeness (density) of the flow of transactions from a particular branch can be checked when data is extracted from the Audit Store;

6.3.2 the interface files in respect of non-Counter transactions, which are inserted into the Branch Database when a Transaction Acknowledgment is accepted by branch staff, are also sent directly to the Audit Store which allows for reconciliation between the two data sources;

6.3.3 when data is taken from the Branch Database to the Audit Store (via the Audit Server) it is sealed and a database of sealed files is maintained so that when data is subsequently retrieved from the Audit Store, its integrity can be checked;

6.3.4 upon receipt of data files retrieved from the Audit Store POL investigators carry out checks to validate data integrity (it should be noted that the nature of these checks was outside the scope of Deloitte's work);

6.3.5 super-user activity is logged; and

6.3.6 super-users cannot amend activity logs, JSNs or invalidated digital seals (i.e. they cannot cover their tracks).

6.4 Although digital signatures did not exist in Legacy Horizon, a "CRC check" was applied which would notify Fujitsu if any amendments had been made to data when it was retrieved from the

POL00029104

audit store if operating correctly. Fujitsu also represented that controls surrounding the Audit Store have remained largely unchanged.

6.5 A branch would not be notified if a super-user amended or deleted a transaction. However, if a change was made in the Branch Database (being the database which holds the live branch accounts used by postmasters):-

6.5.1 before a record of it was "collected" by the Audit Server (which typically happens every 15 minutes), the edition/deletion would track through to the Audit Store. However, if data was subsequently obtained from the Audit Store: (1) deletions would be revealed by the "data density" check (JSNs) [and/or inconsistent interface file records][Deloitte – please confirm that interface file records are also checked at the point of extractions] and (2) edits would be revealed by invalidated digital seals.

6.5.2 if a transaction was edited/deleted after a record of it had been "collected" by the Audit Server it would not impact on the record of the transaction in the Audit Store and there would therefore be a discrepancy between the branch accounts (being the record in the Branch Database) and data subsequently obtained from the Audit Store.

6.6 During testing it was noted that:-

6.6.1 certain super-users can amend activity (audit) logs, JSNs and invalidated digital seals (see executive summary), although it is theorised that they would need to create a computer program to do this in view of the amount of work that would need to be done in a limited window;

6.6.2 the audit trail is only checked when transaction data is extracted from the Audit Store, which typically only happens when POL has cause to investigate specific issue /complaints raised by postmasters;

6.6.3 the data integrity checks that are carried out when data is extracted from the Audit Store can be ignored by Fujitsu staff; and

6.6.4 the audit trail in respect of super-user activity is not pro-actively inspected.

6.7 It ought to be possible for Deloitte to obtain and review the audit logs of super-user access. This work was not originally commissioned as there was no indication of failure in the controls around super-users. Now that the Segregations of Duties issue has been discovered, consideration is being given to whether to conduct this review.

7. GLOBAL USERS

7.1 Global Users are Post Office and Fujitsu staff who have the ability to log on to counter terminals in branches. The existence of Global Users has always been known to Post Office – indeed Global User access is used regularly by field support teams to provide training and conduct audits.

7.2 Some Global Users at Fujtisu have the ability to remotely logon on a branch terminal in order to provide technical support. However, this remote access is "read only" and Deloitte have been unable to find any evidence that this type of access can be used to post or amend transactions.

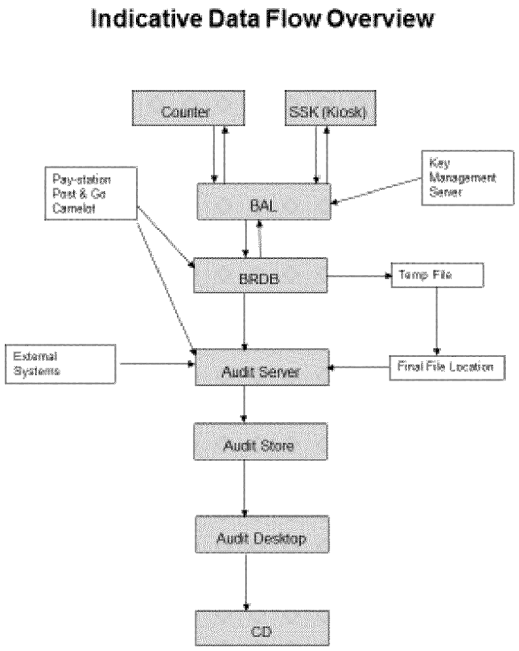
7.3 Other Global Users are able to log on to a terminal whilst physically present in a branch. With this type of access, Global Users are able to conduct transactions. Such transactions will be recorded against the Global User ID (or a new ID created by the Global User) and so are distinguishable from transactions posted by branch staff. Obviously, a postmaster would also know that a person has logged on given that they would be physically present in the branch.

7.4 The above findings are line with pre-existing knowledge of Global Users.

POL00029104

APPENDIX

The high level flow of data from transaction origination through to the Audit Store



System	Description & Detail
Counter	Front end of the system, located behind the 'counter' in Branches. Transactions are input here by the Postmaster.
SSK (Kiosk)	Configured the same way as the Counter, but for Kiosk outlets.
BAL	Transactions are bundled into 'Baskets' and sent from the Counter / Kiosk to the BAL once they are complete. All baskets must balance to 0 (Debit = Credit). Data is then transferred from the BAL – BRDB in real time.
BRDB	The Branch Database is an Oracle database and sits at the heart of the Horizon system. It receives transactions from the BAL and also from other sources as illustrated. Transactions input into BRDB from sources other than the Counter/SSK are fed back to the Counter/SSK and have to be 'Transaction Accepted'.
Audit Server	The Audit Server run a Daemon process which searches for new data in the BRDB. When relevant transactions are identified they are pulled into the Audit Server from the BRDB. Data is held in the Audit Server for approximately 5 days.
Audit Store	After approximately 5 days data is written from the Audit Server to the Audit Store where it is stored semi-permanently (currently 8.5 years of data is stored). Transactional data is stored in a message journal, whereby the completeness of the audit data is confirmed by JSN sequencing.
Audit Desktop	Upon request from POL, Fujitsu audit staff can use the Audit Desktop to query the audit store to extract specified data. Upon extraction from Audit Store – Audit Desktop, the integrity of the data is confirmed via the digital signature and seal check.
CD	A CD is produced with the requested Audit Data.