Strictly confidential, commercially sensitive and legally privileged draft

~~Initial~~ Complaint Review and Mediation Scheme

Horizon Data

Issue

~~Second Sight has asked:~~

Commented [MU1]: I have deleted to remove SS from the equation.

~~"*Can Post Office or Fujitsu edit transaction data without the knowledge of a Subpostmaster?"*~~

This question ~~is~~ often phrased by Applicants i~~a~~s:

"*Can Post Office remotely access Horizon?*"

Phrasing the question in this way does not address the issue that is of concern to Second Sight and Applicants. It refers generically to "*Horizon*" but more particularly is about the transaction data recorded by Horizon. Also, the word "*access*" means the ability to read transaction data without editing it - Post Office / Fujitsu has always been able to access transaction data however it is the alleged capacity of Post Office / Fujitsu to edit transaction data that appears to be of concern. Finally, it has always been known that Post Office can post additional, correcting transactions to a branch's accounts in ways that are visible to Subpostmasters (i.e. Transaction Corrections and Transaction Acknowledgements) - it is the potential for any hidden method of editing data that is of concern.

Thus, this paper addresses the question:

Can Post Office or Fujitsu edit transaction data without the knowledge of a Subpostmaster?"

~~In light of these issues, Second Sight and Post Office have therefore agreed the above reformulation of the question to be addressed.~~

Commented [MU2]: I have deleted to remove SS from the equation.

In summary, Post Office confirms that neither it nor Fujitsu can edit transaction data without the knowledge of a Subpostmaster.

This document

This document provides a generic response to the general question posed above. It is noted that, as yet, neither Second Sight or any Applicant have~~s not~~ presented Post Office with a specific evidenced example of data irregularities or anomalies that may suggest data integrity issues. Nevertheless, Post Office is prepared to investigate incidents alleged by claimants as part of the Complaint and Mediation Scheme providing that is clearly identified (by at least the date, and preferably also the approximate time) in an Applicant's Case Questionnaire Response.

Strictly confidential, commercially sensitive and legally privileged draft

This document has been prepared with the assistance of Fujitsu and the Post Office IT&C Team. Both have approved this document as being accurate.

Response

In simple terms:

- Transactions are recorded in branches by Subpostmasters and their staff.
- The transaction data is transmitted from a branch Horizon terminal to the Post Office data centre.
- At the data centre, the transaction data is stored on a secured server called the Audit Store.
- The transaction data in the Audit Store is what is considered to be the source for "branch's accounts".

There is no functionality in Horizon for either a branch, Post Office or Fujitsu to edit, manipulate or remove a transaction once it has been recorded in a branch's accounts.

The following safeguards are in place to prevent such occurrences:

- Transmission of baskets of transaction data between Horizon terminals in branches and the Post Office data centre is cryptographically protected through the use of digital signatures.
- Baskets must net to nil before transmission. This means that the total value of the basket is nil and therefore the correct amount of payments, goods and services has been recorded in the basket. Baskets that do not net to nil will be rejected by the Horizon terminal before transmission to the Post Office data centre.
- Baskets of transactions are either recorded in full or discarded in full – no partial baskets can be recorded to the Audit Store.
- All baskets are given sequential numbers (known as Journal Sequence Numbers or JSNs) when sent from a Horizon terminal. This allows Horizon to run a check at the Data Centre for missing baskets (which triggers a recovery process) or

additional baskets that would cause duplicate numbers (which would trigger an exception error report to Post Office / Fujitsu).

- All transaction data in the Audit Store is digitally sealed – these seals would show evidence of tampering if anyone, either inadvertently, intentionally or maliciously, tried to change the data within a sealed record.

- Automated daily checks are undertaken on JSNs (looking for missing / duplicate baskets) and on the digital seals (looking for evidence of tampering).

Questions for FJ:

- Is it correct to say that even a malicious attempt to edit transaction data in the audit store would leave a footprint?

- When data is retrieved from the audit store, are the digital seals and JSNs checked every time?

Although once recorded a transaction cannot be edited or deleted, transactions (including negative transactions) can be **added** to a branch's accounts in the following ways only:

Are the three ways below, the only ways to affect a branch's accounts?

1 In branch

Branch staff record additional transactions during their normal daily use of Horizon. So long as they are logging on with their own unique User ID and not sharing User IDs and passwords within a branch, each transaction will be logged against the user's own User ID.

Horizon does not include functionality that allows either Post Office or Fujitsu to log on to a branch terminal of Horizon remotely in order to edit transactions recorded by Branch staff. It is possible for Fujitsu to view branch data in order to provide support and conduct maintenance but this does not allow access to any functionality that could be used to edit branch data.

Questions for FJ:

- Is the above statement correct? No; we cannot log on to a branch remotely

- What assurances are in place that this support access cannot be misused in order to conduct transactions in branch?

Commented [DJ3]: The system has been designed so that transaction data cannot be edited, only new transactions added via standard operating processes. All access to systems are logged and access is segregated following ISO27001 principles (this is audited annually).

MU - so it is correct in a sense as it is not possible to edit data and any malicious additional transactions, by the nature that they are added, would therefore leave at least some kind of footprint.

Commented [GT4]: Again essentially yes. It would be possible for us to retrieve data from the audit store without doing these checks, but if the data is being used in support of a prosecution or such like then these checks are always made.

Commented [MU5]: FJ to provide an answer. I presume the answer is yes

- The following responses highlighted in green refer to any attempts to change the data/transactions by someone in the data centre.

Commented [MU6]: The below assurances need to be provided in more detail. Examples, detailed by response, below:

- 1. The system is designed to prevent it

Commented [MU7]: How? Can we give a 'walked through' example of how the systems design prevents misuse?

- 2. The system is designed to leave a footprint of actions taken by support staff.

Commented [MU8]:
What does this footprint look like?
What (footprint) variations exist?

- 3. The audit trail for transactions coming from the branch would be inconsistent with the branch accounts.

Commented [MU9]:
Can we describe what typical branch data looks like VS data that would be considered inconsistent?

When inconsistent data is apparent / suspected (How?) – what is the subsequent process?

There is the capability for Post Office employees to log on to a branch terminal locally (i.e. by being physically in a branch) using a new User ID and password and then conduct transactions. This would only be done in special circumstances (such as when defunding a branch following a branch closure). Any transactions conducted would be recorded against that new User ID and not against the User ID of any branch staff.

Questions for POL / FJ:

- What controls are in place to make sure that the above local access is not misused?
- This is for POL to answer - not FS.

Commented [MU10]: Noted – I will find this out

2 TAs and TCs

Post Office can send transaction acknowledgements (**TA**) or transaction corrections (**TC**) to branches. TAs are used to record transactions that have been processed in branch through other systems (eg. the sale of Lottery products on the Camelot terminal) and TCs to correct errors made by branches.

Both TAs and TCs need to be accepted by a user logged into the branch Horizon terminal before they are recorded in the branch accounts. They are therefore fully visible to each branch.

3 Balancing Transactions

Fujitsu (but not Post Office) can manually inject a new transaction into a branch's accounts using the Balancing Transaction Process. This process is used in the event of an accounting error that cannot be corrected by use of a TA or TC and it is in accordance with good industry practice to have functionality of this nature in a system like Horizon.

I believe that we have only ever done one of these 'Balancing Transactions' so we would have to discuss that as a specific. The need to do so was triggered by a bug in the code which meant that there was no way to bring the system to a correct state without intervening at a very low level. This whole process was agreed with POL.

I think the questions below are not of any real value given the above.

FJ – What is the effect of a Balancing Transaction?

- o What types of transaction can it add?
- o Does it add a transaction or an entirely new basket?
- o Can it add a transaction to an existing basket?
- o If a new basket, does the new basket get a new JSN? How does this not clash with the JSNs generated by the branch terminal?
- o Where does the BT take affect? If it makes changes in the Audit Store, how is this change communicated (if at all) back to the records held on the branch terminal?
- o Does the BT affect the branch's cash and stock holdings?
- o Does the BT affect the branch's end of trading period balance?

The use of this process is strictly controlled by Post Office. For a transaction to be manually injected:

- o FJ – please describe the process and controls in place for use of this process?

These access controls meet industry good practice standards and are audited under ISO27001 and by LINK (the industry body for ATMs) and PCI (card payment compliance).

Injected Balancing Transactions are visible in the branch's accounts and so the injected transaction will be visible to a Subpostmaster. The transaction is also attributed to a unique transaction ID used only for these type of transactions. It is not recorded against the User ID of any member of branch staff.

FJ – Is this correct?

- o When are SPMRs made aware that an injection is to occur? Before or after it has been injected?
- o How are Balancing Transactions visible to a branch?
- o Can a transaction be added to any trading day?
- o If so, can a transaction be added to a day more than 60 days ago?

Commented [MU11]: Further to the final question in this paper

"FJ – the above information is based on an email from John Simpkins to Deloitte in May 2014 – please confirm that this is correct?"

Could we be provided with all the information related to this incident so that we can judge, once we pull together all the information supplied together, whether or not the below questions still require bottoming out?

Commented [DJ12]: Note – it is not possible to edit existing transaction / basket data as detailed earlier.

Commented [DJ13]: These are new transactions with unique jsn's and identifiers

Commented [DJ14]: Note – there are no records held on a branch terminal.

Commented [DJ15]: See details of incident in March 2010 for details on how this process works

Commented [DJ16]: Same as above

Commented [DJ17]: See incident in March 2010 for details

WBON0000327

- If so, given that branches can only see 60 days of data on their terminals, how would a Balancing Transaction be visible to a branch?

This process is materially the same for Horizon and Horizon Online.

This use of Balancing Transactions is incredibly rare. Within the Audit Store is an audit log that automatically records any use of Balancing Transactions. This log shows that a Balancing Transaction has only be used once in the last 7 years (being the retention period for the log). A Balancing Transaction was injected on 3 March 2010 and only affected one branch (FAD code: 226542 - which is not a branch under review in the Scheme).

FJ – the above information is based on an email from John Simpkins to Deloitte in May 2014 – please confirm that this is correct?

Post Office Limited

DATE