Strictly confidential and commercially sensitive

Initial Complaint Review and Mediation Scheme

Horizon Data

Issue

Second Sight has asked whether Post Office or Fujitsu can edit Horizon transaction records 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, Second Sight has not presented Post Office with a specific example of a "remotely generated transaction". For the reasons stated below, it would be surprising if such a transaction was raised as part of the Scheme. Nevertheless, Post Office is prepared to investigate any suspected transaction of this nature that is clearly identified (by at least the date, and preferably also the approximate time, of the transaction) in an Applicant's Case Questionnaire Response.

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

There is no functionality in Horizon for either a branch, Post Office or Fujitsu to delete or alter a transaction recorded in a branch's accounts.

Safeguards are also in place to ensure that no transactions are lost, altered or improperly added to a branch's accounts:

- Transmission of transaction data between Horizon terminals and the Post Office data centre is encrypted.

- 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 transacted. 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

- All baskets are given sequential numbers when sent from a Horizon terminal. This allows Horizon to run a check 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).

- Transaction data is stored on a secure audit server. All transaction data 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.

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:

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 id.

2 TAs and TCs

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

Fujitsu (but not Post Office) can manually inject a new transaction into a branch's accounts. This process is used in the event of an 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.

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

- A formal change order request from the Post Office IT team to Fujitsu must be approved by both parties. [Correct? Does this come from IT&C?]
- Two people at Fujitsu must approve the manual change before it is processed (a "four eyes" sign off).
- The user at Fujitsu conducting the sign off must log-on to the system using two factor authentication.

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 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.

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

This use of manually injected transactions is incredibly rare - it has only be used once during the life of Horizon Online (ie. since January 2010). The unique identifier recorded against injected transactions can be easily identified within the transaction logs of Horizon Online. Fujitsu has reviewed these transaction logs and identified that the manual injection process was used once in March 2010 during the roll out of the pilot for Horizon Online and affected only [number of branches / FJ to provide the name of the branches]. None of these branches have made applications to the Scheme [AP to confirm once affected branches are known].

[FJ - please explain the effect of the injected transaction in March 2010 and, if possible, why this was done]

It is technically possible to also confirm whether a manually injected transaction has occurred on the old Horizon system (subject to retention periods of branch transaction logs). However, this exercise is considerably time consuming. In the absence of any credible evidence that this process has been misused, it would be disproportionate to undertake this exercise at this stage.

Given that this process is rarely used, and the potential resolve nearly all branch accounting issues through TAs and TCs, Post Office considers that it would be extraordinarily unlikely that it would ever commission the injection of a transaction into the Horizon system without first notifying the affected branches.

[Do we know whether the branches affected in 2010 were notified of the injected transaction?]