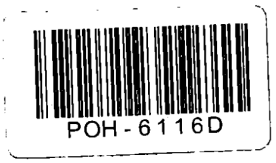
FUJ00155371

Thomas Penny

Subject: Updated: Audit Strengthening CP Review/Refresh
Location: Sorting Room - RMGA TEAM ONLY (2nd Floor - Room 03)

Start: Wed 26/11/2008 11:30
End: Wed 26/11/2008 12:00
Show Time As: Tentative



Recurrence: (none)

Meeting Status: Not yet responded

Required Attendees: Evans Steve (FEL01); Sewell Peter (FEL01); Hodgkinson Allan AJ; Thomas Penny

Audit Strengthening CP Review/Refresh

Sorting Room - RMGA TEAM ONLY (2nd Floor - Room 03)

Attached: my precis with Alan's comments
Plus a standard ARQ form....

Standard_Fuj_ARQ _WS_V7 .doc (1...

Audit_Str_CP_Preci s(v0 1-AH).d...

FUJ00155371

HNGx CP – Strengthen the HNGx Audit Solution, and enable analysis of Counter Event messages.

Originator:	Alan Holmes
Change Owner:	Pete Sewell
Technical Sponsor:	Alan Holmes

The Audit System and ARQ (Audit Record Queries) Service

- We are contractually obliged to support the Prosecution Support Service via CS, and provide historical extracts of data from the Audit archive (7yrs data), used in legal proceedings often to prove accusations of fraud against Postmasters.
- The completeness of the data extracts provided is assumed, and witness statements state as much (see last page).
- The service has worked by providing extracts of Riposte messagestore data only.
- This service (worth the best-part of the annual £850k security revenue - PS) will remain to 2015 and beyond.

Comment [AH1]: It is more than 'assumed' or at least so we thought.
The Riposte sequence numbers are checked for gaps & from this we assert that the extract shows a tru e& complete representation of what happened at the branch.

Problem

- PC0152376 highlighted that in certain error conditions in the EOD process Riposte cannot be relied upon to write a consistent set of messages to the local store.
- This particular issue has been fixed (Dev: PC0164429 / Release: PC0165710, currently being distributed to Live), but it is very probable that similar problems exist in the Horizon system.
- Therefore the process of providing data now needs to include the extraction and cross-checking of Event data to help identify where data integrity might be compromised.
- The statements currently asserted in Witness Statement cannot be guaranteed in all cases (even after this CP) (see example on last page) but this CP seeks to strengthen the process and allow us to reliably identify where the assertion can or cannot be made.

Comment [AH2]: Also worth stressing that we can't retrospectively fix the data held in the Audit archive

Deleted: not be complete

Current Process

- Many manual steps, requiring great care and skill from individual resources, obvious potential for human error .
- Data distributed or transferred over too many platforms/media: inherently insecure.
- Tactical solution, post PC0152376 has introduced further manual steps.

Solution

- Manual process needs to be automated wherever possible for a permanent HNGx solution
- Reduce the steps in the process, and over time allow the refinement of filters used during event extraction, reducing the overall data load and task.
- We cannot totally automate the process; we require permanent skilled part-time resource to perform the events-analysis.

Deleted: application

Deleted: to both txn and

Deleted: to

Deleted: process and

Deleted: 00/00/0000 00:00:00

Deleted: 24/10/2008 15:32

FUJ00155371

HNGx CP – Strengthen the HNGx Audit Solution, and enable analysis of Counter Event messages.

Originator: Alan Holmes
Change Owner: Pete Sewell
Technical Sponsor: Alan Holmes

Costs

- Current costs (of skilled resource, scheduled to leave end of Nov)
  - Extraction, filtering, manual work - **1.5d/ week**
  - Event extraction, checking and analysis – **2d/week** (currently performed by Gareth Jenkins/Anne Chambers)
- Strengthening and Automation of process via this CP
  - 55md
- Ongoing costs (Post CP)
  - Extraction, filtering, manual work - **0.5d/ week**
  - Event extraction, checking and analysis – **2d/week** (performed by identified resource), ***possibly reducing to 1d/week as filters are extended***

Comment [AH3]: Resource in the first bullet only is leaving

Benefit/Risk

- Strengthen the process or weaken the witness statement in all cases
- If we cannot better identify where data integrity can or cannot be guaranteed, then we are in breach of contract and may:
  - Be fined heavily
  - Not be able to offer the ARQ service, or will undermine confidence in the service.
- We need to reduce the reliance on current skilled resource, and make the process imminently transferable
- Reduce on-going cost of the parts of the process which are manual, and automate the use of filters to allow that reduction to continue

Witness Statement extract:

An audit of all information handled by the TMS is taken daily by copying all new messages to archive media. This creates a record of all original outlet transaction details including its origin - outlet and counter, when it happened, who caused it to happen and the outcome. The TMS journal is maintained at each of the Fujitsu Services Data Centre sites and is created by securely replicating all transaction records that occurred in every Outlet. They therefore provide the ability to compare the audit track record of the same transaction recorded in two places to verify that systems were operating correctly. **Records of all transactions are written to audit archive media.**

Deleted: 00/00/0000 00:00:00
Deleted: 24/10/2008 15:32

FUJ00155371

Witness Statements.

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Statement of

Age if under 18 Over 18 (If over 18 insert 'over 18')

This statement (consisting of pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe true.

Dated the day of 2008

Signature

I have been employed by Fujitsu Services, Post Office Account, formally ICL Pathway Ltd since DATE as an Information Technology (IT) Security Analyst responsible for audit data extractions and IT Security. I have working knowledge of the computer system known as Horizon, which is a computerised accounting system used by Post Office Ltd. I am authorised by Fujitsu Services to undertake extractions of audit archived data and to obtain information regarding system transactions recorded on the Horizon system.

Horizon's documented procedures stipulate how the Horizon System operates, and while I am not involved with any of the technical aspects of the Horizon System, these documented processes allow me to provide a general overview.

At each Post Office there are counter positions that have a computer terminal, a visual display unit and a keyboard and printer. This individual system records all transactions input by the counter clerk working at that counter position. Clerks log on to the system by using their own unique password. The transactions performed by each clerk, and the associated cash and stock level information, are recorded by the computer system in a stock unit. Once logged on, all transactions performed by the clerk must be recorded and entered on the computer and are accounted for within the user's allocated stock unit.

Formatted: Marching Red Ants, Highlight

The Horizon system provides a number of daily and weekly records of all transactions input

Formatted: Marching Red Ants, Highlight

Signature Signature witnessed by

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

into it. It enables Post Office users to obtain computer summaries for individual clients of Post Office Limited e.g. Alliance & Leicester. The Horizon system also enables the clerk to produce a periodic balance of cash and stock on hand combined with the other transactions performed in that accounting period, known as a trading period.

Where local reports are required these are accessed from a button on the desktop menu. The user is presented with a parameter driven menu, which enables the report to be customised to requirements. The report is then populated from transaction data that is held in the local database and is printed out on the printer. The system also allows for information to be transferred to the main accounting department at Chesterfield
The Post Office counter processing functions are provided through a series of counter applications: the Order Book Control Service (OBCS) that ascertained the validity of DWP order books before payment was made, this application ceased in June 2005; the Electronic Point of Sale Service (EPOSS) that enables Postmasters to conduct general retail trade at the counter and sell products on behalf of their clients; the Automated Payments Service (APS) which provides support for utility companies and others who provide incremental in and out payment mechanisms based on the use of cards and other tokens and the Logistics Feeder Service (LFS) which supports the management of cash and value stock movements to and from the outlet, principally to minimise cash held overnight in outlets. The counter desktop service and the office platform service on which it runs provides various common functions for transaction recording and settlement as well as user access control and session management.

Information from counter transactions is written into a local database and then replicated automatically to databases on all other counters within a Post Office outlet. The information is then forwarded over ADSL (Asymmetric Digital Subscriber Line)or other communication service, to databases on a set of central Correspondence Servers at the Fujitsu Services data centres. This is undertaken by a messaging transport system within the Transaction Management Service (TMS). Various systems then transfer information to Central Servers that control the flow of information to various support services. Details of outlet transactions are normally sent at least daily via the system. Details are then forwarded daily via a file transfer

Formatted: Marching Red Ants, Highlight

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

service to the Post Office accounting department at Chesterfield and also, where appropriate, to other Post Office Clients.

An audit of all information handled by the TMS is taken daily by copying all new messages to archive media. This creates a record of all original outlet transaction details including its origin - outlet and counter, when it happened, who caused it to happen and the outcome. The TMS journal is maintained at each of the Fujitsu Services Data Centre sites and is created by securely replicating all transaction records that occurred in every Outlet. They therefore provide the ability to compare the audit track record of the same transaction recorded in two places to verify that systems were operating correctly. Records of all transactions are written to audit archive media.

Formatted: Marching Red Ants, Highlight

Formatted: Marching Red Ants, Highlight

Formatted: Marching Red Ants, Highlight

Formatted: Marching Red Ants, Highlight

The system clock incorporated into the desktop application on the counter visual display units is configured to indicate local time. This has been the situation at (INSERT PO), Branch Code (INSERT) since (INSTALLATION DATE) when the Horizon system was introduced at that particular Post Office.

The Horizon system records time in GMT and takes no account of Civil Time Displacements, thus during British Summer Time (BST) (generally the last Sunday in March to the last Sunday in October), system record timings are shown in GMT – one hour earlier than local time (BST).

There was, however, one exception which related to the category of transactions 'Transfer In' where events recorded in the Transaction Logs, were shown in local time. This meant that during the designated summer months 'Transfer In' log entries were recorded in BST instead of GMT and showed a one hour forward displacement in time from other transactions being recorded in the logs. This anomaly was corrected during the winter months prior to BST 2005 since when 'Transfer In' log entries have been recorded in GMT, consistent with all other transactions being recorded in the logs. – Delete this for data post Oct 2004.

Formatted: Font color: Red

When information relating to individual transactions is requested, the data is extracted from the

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

audit archive media via the Audit Workstations (AW's). Information is presented in exactly the same way as the data held in the archive although it can be filtered depending upon the type of information requested. The integrity of audit data is guaranteed at all times from its origination, storage and retrieval to subsequent despatch to the requester. Controls have been established that provide assurances to Post Office Internal Audit (POIA) that this integrity is maintained.

Formatted: Marching Red Ants, Highlight

Formatted: Marching Red Ants, Highlight

During audit data extractions the following controls apply :

1. Extractions can only be made through the AWs which exist at Fujitsu Services, Lovelace Lane, Bracknell, Berkshire and Fujitsu Services, Sackville House, Brooks Close, Lewes, East Sussex. These sites are both subject to rigorous physical security controls appropriate to each location. All AWs are located in a secure room subject to proximity pass access within a secured Fujitsu Services site.
2. Logical access to the AW and its functionality is managed in accordance with the Fujitsu Services, Post Office Account Security Policy and the principles of ISO 17799. This includes dedicated Logins, password control and the use of Microsoft Windows NT security features.
3. All extractions are logged on the AW and supported by documented Audit Record Queries (ARQ's), authorised by nominated persons within Post Office Ltd. This log can be scrutinised on the AW.
4. Extractions are only made by authorised individuals.
5. Upon receipt of an ARQ from Post Office Ltd they are interpreted by CS Security. The details are checked and the printed request filed.
6. The required files are identified and marked using the dedicated audit tools.
7. Checksum seals are calculated for audit data files when they are written to audit archive media and re-calculated when the files are retrieved.
8. To assure the integrity of the audit data while on the audit archive media the checksum seal for the file is re-calculated by the Audit Track Sealer and compared to the original value calculated when the file was originally written to the audit archive media. The result is maintained in a Check Seal Table.

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

9. The specific ARQ details are used to obtain the specific data.
10. The files are copied to the AW where they are checked and converted into the file type required by Post Office Ltd.
11. The requested information is copied onto removal CD media, sealed to prevent modification and virus checked using the latest software. It is then despatched to the Post Office Ltd Casework Manager using Royal Mail Special Delivery. This ensures that a receipt is provided to Fujitsu Services confirming delivery.

ARQ(NUMBER) was received on (DATE) and asked for information in connection with the Post Office at (NAME), Branch code (NUMBER). I produce a copy of ARQ(NUMBER) as Exhibit (INITIAL/NUMBER). I undertook extractions of data held on the Horizon system in accordance with the requirements of ARQ(NUMBER) and followed the procedure outlined above. I produce the resultant CD as Exhibit (INITIAL/NUMBER). This CD, Exhibit (INITIAL/NUMBER), was sent to the Post Office Investigation section by Special Delivery on (DATE).

The report is formatted with the following headings:

ID – relates to counter position
User – Person Logged on to System
SU – Stock Unit
Date – Date of transaction
Time – Time of transaction
SessionId – A unique string relating to current customer session
TxnId – A unique string relating to current transaction
Mode – e.g. SC which translates to Serve Customer
ProductNo – Product Item Sold
Qty – Quantity of items sold
SaleValue – Value of items sold
Entry method - Method of data capture for Transactions (0 = barcode, 1 = manually keyed, 2 = magnetic card, 3 = smartcard, 4 = smart key)
State – Relates to OBCS

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

IOP - Order Book Number – OBCS only

Result – Order Book Transaction Result – OBSC only

Foreign Indicator – Indicates whether OBCS payment was made at a local or foreign outlet (0- Local, 1- Foreign). The foreign indicator defaults to a '0' for all manually entered transactions - OBCS only

The Event report is formatted with the following headings:

Groupid – FAD code

ID – relates to counter position

Date – Date of transaction

Time – Time of transaction

User – Person Logged on to System

SU – Stock Unit

EPOSSTransaction.T – Event Description

EPOSSTransaction.Ti – Event Result

(FOR MULTIPLE DATA PROVIDED BOTH BEFORE AND AFTER 24 JANUARY 2006 (FROM ARQ562/0506) INCLUDE THE FOLLOWING PARAGRAPH. FOR DATA PROVIDED WEF 24 JANUARY 2006 AND FROM ARQ562/0506 DELETE THIS PARA BUT INCLUDE THE ADDITIONAL HEADINGS BELOW)

Formatted: Not Highlight

In January 2006 a change was made to the original extract query to include additional records from the raw audit data. In particular, this refined query now includes details of Inactivity Logouts, Authority Logouts and Failed Logins. It should be noted that no changes were made to the original Audit data but just to the selection of records from the Audit for presentation to Post Office Limited in the ARQ Spreadsheet. ARQs LIST have this additional data.

Type – Inactivity Logout noted

Logout Authority – User who logged out the account

SecurityEvent.User – User who failed to log in

Signature

Signature witnessed by

FUJ00155371

Witness Statement

(CJ Act 1967, s9; MC Act 1980, ss 5A(3)(a) and 5B, MC Rules 1981, r 70)

Continuation of statement of

There is no reason to believe that the information in this statement is inaccurate because of the improper use of the computer. To the best of my knowledge and belief at all material times the computer was operating properly, or if not, any respect in which it was not operating properly, or was out of operation was not such as to effect the information held on it.

Formatted: Marching Red Ants, Highlight

Any records to which I refer in my statement form part of the records relating to the business of Fujitsu Services. These were compiled during the ordinary course of business from information supplied by persons who have, or may reasonably be supposed to have, personal knowledge of the matter dealt with in the information supplied, but are unlikely to have any recollection of the information or cannot be traced. As part of my duties, I have access to these records.

Signature

Signature witnessed by