FUJ00122457

Document Title: MANAGEMENT OF THE PROSECUTION SUPPORT SERVICE FOR AUDIT RECORD QUERIES

Document Type: Procedure

Release: N/A

Abstract: This document outlines the end-to-end procedures required to manage and deliver the Prosecution Support Service for Audit Record Queries

Document Status: Draft

Originator & Dept: Penny Thomas (CS Security)

Contributors: Alan Holmes

Internal Distribution: Pete Sewell, Andy Dunks

External Distribution: Dave Posnett, Post Office Limited, Security Team

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Naomi Elliott	CS Director		
Pete Sewell	CS Deputy Security Manager		

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/Peak
0.1	11/02/02	Initial Draft	
0.2	24/10/02	Incorporation of comments after initial review. Amendment to signed contract.	
0.3	15/11/02	Incorporate comments after review	
1.0	26/11/02	Version for approval	
1.1	02/02/05	Update to reflect current changes	
2.0	29/02/05	Version for approval	
2.1	6/06/07	For approval after review	

0.2 Review Details

Review Comments by :	
Review Comments to :	Penny.Thomas@ GRO & RMGADocumentmnagement@ GRO) GRO

Mandatory Review	
CS Deputy Security Manager	Pete Sewell
Optional Review	
Audit	Alan Holmes
Senior Commercial Manager	Hilary Forrest
*Issued for Information – **Please restrict this distribution list to a minimum***	
Position	*Name*
Post Office Limited, Security Team	Dave Posnett

(*) = Reviewers that returned comments

0.3 Associated Documents

FUJ00122457

Reference	Version	Date	Title	Source
PA/TEM/001	8.0	19/12/02	Fujitsu Services Document Template	PVCS
CR/FSP/006			Audit Trail Functional Specification	
CS/SER/016			Service Description for the Security Management Service	
IA/PRO/004			Audit Data Extraction Process	

Unless a specific version is referred to above, reference should be made to the current approved versions of the document

0.4 Abbreviations/Definitions

Abbreviation	Definition
Audit Record Query (ARQ)	A Record Query that is not a Banking Transaction Record Query and which relates to Transactions.
Banking Record Query	A Record query in respect of a Banking Transaction which the Data Reconciliation Service has reconciled or has reported as an exception, the result or records of which are subsequently queried or disputed by Post Office Ltd or a third party.
CS	Customer Services
Banking Transaction Record Query	A Record Query in respect of a Banking Transaction which the Data Reconciliation Service has reconciled or has reported as an exception, the result or records of which are subsequently queried or disputed by Post Office Ltd or a third party
Branch Code	A Post Office outlet unique identifier.
HSH	Horizon System Helpdesk
Prosecution	Civil or criminal court or statutory tribunal proceedings related to Transactions or fraudulent actions conducted at a Post Office Outlet
Old Format Queries	The extraction of records created before commencement of Network Banking Pilot (Soft Launch) relating to Transactions (other than Banking Transactions) meeting the Search Criteria, such extraction being limited to the following specific types of information/data fields: the ID for the user logged-on, Counter Position ID, stock unit reference, Transaction ID, Transaction start time and date, Customer Session ID, mode (e.g. serve customer),

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

	product number and quantity, and sales value
POL	Post Office Limited
PSS	Royal Mail Group Account Prosecution Support Section
PSS Day	Between 09:00 and 17:30 Monday to Friday excluding English Bank Holidays.
Record Query	The extraction of records created after commencement of Network Banking Pilot (Soft Launch) in accordance with the terms paragraph 7.3 of N01 relating to Banking Transactions and, in the case of Audit Record Queries relating to all Transactions meeting the Search Criteria, such extraction being limited to specific types of information/data fields.
Audit Record Query Form	The form used by POL to request detailed transaction data.
Rolling Year	Any Record Queries received over the yearly limit shall be seen as the following year's requests and as such will not be processed until the following year. In other words, they will be rolled over in to the following year's requests.
Search Criteria	Means either of: (a) date range (not exceeding 31 consecutive days), Outlet and PAN(or equivalent identifier); or (b) date range (not exceeding 31 consecutive days), and Outlet, which may be specified for an Audit Record Query. NB this is different from the criteria used for Banking Transactions Record Queries

0.5 Changes in this Version

Version	Changes
2.0	Update to reflect new ARQ contract details Minor typo errors Minor changes to internal work processes
2.1	For approval after review

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

0.6 Changes Expected

Changes

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

Table of Contents

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

1.0 Introduction

The Network Banking Prosecution Support Service was introduced in response to Network Banking Requirements 260 and 315. The scope of the Service is outlined in CS/SER/016.

This document was intended to assist the management and delivery of the service necessary to support Post Office Ltd in respect of criminal prosecution or civil litigation for the Horizon solution.

Audit Record Query requests are received, documented, extracted from the Audit Archive and progressed to resolution, as is the production of evidence and witness statements in support of prosecutions.

This document is without prejudice to any of the parties and nothing contained herein shall be deemed or construed as affecting contractual obligations or creating new contractual obligations between any of the parties.

©Copyright Fujitsu Services Ltd 2007

FUJ00122457

2.0 Scope

This document sets out the procedures to be adopted by the Royal Mail Group Account's Prosecution Support Section (PSS) for managing and dealing with Audit Record Queries (ARQs) for investigation and prosecution support purposes, including the:

- Undertaking of ARQs;
- Presentation of transaction records extracted by ARQs;
- Analysis of appropriate records and logs;
- Preparation of witness statements of fact in relation to ARQs;
- Attendance at Court by relevant employees to give evidence in respect of witness statements;
- Undertaking of additional litigation/prosecution support activities as may be requested on a case-by-case basis on the instruction of Legal Counsel.

It is recognised that it is not always possible to deliver a standardised response to all prosecution related ARQs. However, a comprehensive set of standard data information requests have been agreed and have proven to satisfy the majority of cases. The exceptions are dealt with on a case by case basis. These procedures can therefore provide a flexible approach to the provision of prosecution support.

ARQs in support of potential prosecutions will be obtained solely from the Horizon System Audit Archive / Server. The method by which the integrity of this data is protected is described in the Audit Trail Functional Specification. Evidence in support of data integrity will be sourced from Audit Archive / Server and the Royal Mail Group Account's business logs. All access to audit data is restricted to named individuals via dedicated workstations located in a secure environment. Supporting evidence is sourced from relevant business records and logs.

Requests for Information will fall into two general categories:

- Audit Record Query

  This involves the extraction from the audit archive of records relating to data for a particular outlet.

- Witness Statement.

  This request requires the provision of a witness statement of fact in support of data extracted or records reviewed.

FUJ00122457

3.0 Audit Record Queries

3.1 Scope

An ARQ is an extraction from the Audit Archive of records relating to transactions which meet specific search criteria. ARQs may be undertaken to provide transaction and other details required to facilitate an investigation or in support of a prosecution.

Throughout this document the term Audit Record Query is used to refer to an extraction of data from the Audit Archive.

3.2 Limits on Audit Record Queries.

The number of ARQs requested by Post Office Ltd in connection with investigation or prosecution shall be as referenced in the Service Description for the Security Management Service CS/SER/-16.

3.3 Search Criteria

The search criteria for ARQs in support of prosecution are either:

(a) Date or dates (not exceeding 31 consecutive days), Outlet and PAN (or equivalent identifier)

Or;

(b) Date or dates (not exceeding 31 consecutive days), and Outlet.

which may be specified for an ARQ.

Each ARQ shall cover a date range of up to and including 31 consecutive days. Individual dates or multiple date ranges can be accommodated provided that the overall timeframe requested does not exceed 31 consecutive days for each ARQ.

Each ARQ shall relate only to an individual Outlet.

Audit Record Queries are limited to specific types of information/data fields these are:

- the ID for the user logged-on,
- Counter Position ID,
- stock unit reference,
- Transaction ID,
- Transaction start time and date,
- Customer Session ID,

FUJ00122457

- mode (e.g. serve customer),
- product number,
- product quantity,
- sales value.

Royal Mail Group Account will consider reasonable requests from Post Office Ltd. for a variation to the requested information/data fields. Such variation requests should be specified in the relevant ARQ form.

3.4 Format for Audit Record Query Requests

ARQs in connection with prosecutions shall be made via the Audit Record Query Form.

Post Office Ltd will specify the following details for each ARQ:

- Date of request
- Outlet name and Branch code
- Date range, the maximum date range for each ARQ is 31 consecutive days.
- General requirements. This includes the required attributes associated with the ARQ.
- Output format required. This is normally a standard Excel 97 version with separate columns for each attribute requested.

Each ARQ shall be allocated a unique identifier to facilitate the logging and monitoring of work carried out. The identifier shall be "ARQ" followed by a sequential number starting from 1 (1 to nnnn) for each financial year. This will provide the audit trail information necessary to ensure continuity of evidence if required later at a court or tribunal.

The agreed Audit Record Query (ARQ) Form is at Appendix 1.

3.5 Exclusions

ARQs in connection with Disputed Banking Transactions are not covered in this document. Refer to NB/PRO/002.

3.6 Audit Record Query Resolution Time Scales

The resolution timeframes for ARQs shall be as referenced in the Service Description for the Security Management Service CS/SER/-16.

FUJ00122457

4.0 Prosecution Support

4.1 Scope

The Royal Mail Group Account shall, in relation to an ARQ and at the request of Post Office Ltd:

- Analyse appropriate Horizon Help Desk calls, as requested
- Analyse fault logs for the devises from which the records of transactions were obtained
- Provide witness statements of fact in relation to an ARQ
- Attend Court in order to give evidence in support of a witness statement.

4.2 Exclusions

The provision of additional prosecution support is excluded from the service detailed above. Additional prosecution support is covered in Section 8 Additional Prosecution Support.

FUJ00122457

5.0 Notification Process

5.1 Contact Points

5.1.1 Post Office Ltd

All ARQs in conjunction with investigation and or prosecution must be authorised by the Post Office Ltd Security Team.

Requests will be accepted only from the Post Office Ltd's Casework Manager or his deputy.

The Post Office Ltd Casework Manager will advise the Royal Mail Group Account's Prosecution Support Manager, or his deputy, of named deputies, authorised to request ARQs.

5.1.2 The Royal Mail Group Account

Post Office Ltd will submit all requests for ARQs in connection with investigation and prosecution to:

Customer Service Prosecution Support Section,

Fujitsu Services

Lovelace Road

Bracknell

Berkshire RG12 8SN

The Audit Record Query will be sent via email to the nominated team.

5.2 Request Process

Post Office Ltd will complete an ARQ form and email it to the nominated team. The details of the request and the date of receipt shall be recorded in the Prosecution Support Database.

Post Office Ltd will also keep a log of all requests made to the PSS.

FUJ00122457

6.0 Management Process

6.1 Continuity of Evidence

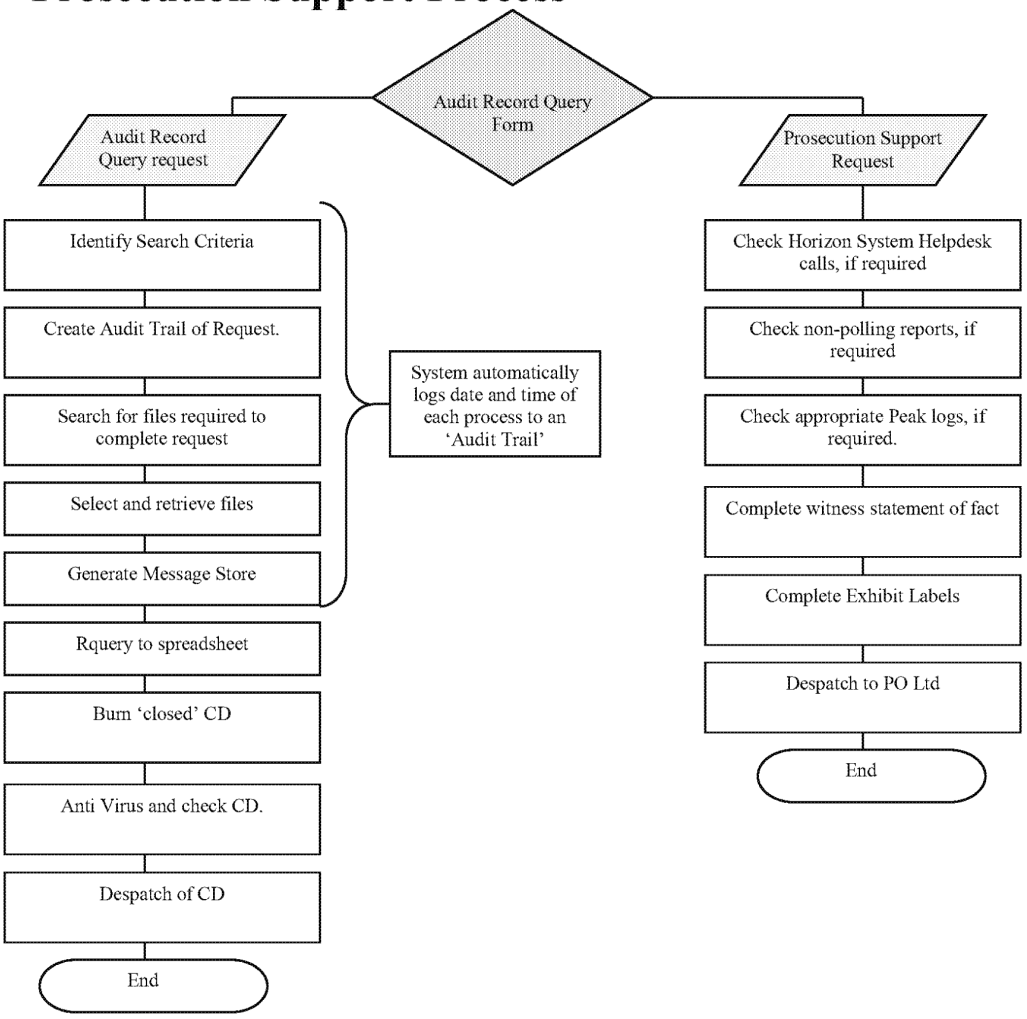
Where possible a member of the PSS Team will undertake the entire end to end prosecution support process.

6.2 Prosecution Support Database

The Database shall track when the request was received, the SLA return timeframe, who completed the request, when it was started and when it was completed, who checked the data and when the disc was posted to POL.

FUJ00122457

Prosecution Support Process



FUJ00122457

7.1 Audit Record Query

7.1.1 Identify Search Criteria

The team member allocated to the request shall identify the search criteria from the ARQ form.

7.1.2 Create Audit trail of request

The Horizon Audit System provides an audit trail. The audit trail records the date and time of each process carried out on the Horizon Audit System to complete the ARQ. The search criteria and ARQ identifier shall be used to create the directory structure of each audit trail. An audit trail is produced only when an ARQ is marked as completed on the Extractor Client. (The audit trail is not the Prosecution Support Database). The audit trail is used to attest to the integrity of data held on the Horizon Audit System and data extracted for ARQs.

The Prosecution Support Database holds information relating to when the ARQ was received, the SLA return date, who completed the request, when they started and completed the request, who checked the data and when the disc was sent to POL.

7.1.3 Search for files required to complete request

A search for files required to complete the request shall be initiated using the audit extractor GUI.

7.1.4 Select and retrieve files

Once the search has completed and returned the results each required file shall be marked for selection and then selection will be initiated. Files extracted to the server shall be seal checked as they are extracted. This check confirms that the data has not been altered from the time the transaction first originated to the time it was stored. After the files have been extracted the operator shall check the seal status and ensure all seals match.

7.1.5 Generate messagestore

A messagestore of the selected files shall be initiated on the operator's local machine using the files extracted to the audit server.

7.1.6 Rquery to spreadsheet

Once the messagestore has been successfully generated, the Rquery tool shall be used to select the files as per the search criteria set out in the ARQ. The Transaction records extracted for the ARQ are exported by the Rquery tool to an Excel 97 Format.

FUJ00122457

7.1.7 Encryption of Data

It is a mandatory requirement of PCI that all sensitive data communicated either by disc or e-mail is to be encrypted. The PGP SDA Encryption tool has been selected as the most appropriate. All data supplied by CS Security will be subject to PGP Encryption. Full details can be found in IA/PRO/004.

7.1.8 Burn closed CD-W

Once the data is complete and formatted it shall be burnt to 'closed' CD-W along with a word document that shall provide an explanation of the format in which the data is provided. The CD-W will be labelled, and written on the label shall be the ARQ reference number, the Branch name and code, the SLA due date, the name of the PSS employee who compiled the data and the date it was completed, the date range requested and the name of the PSS employee who checked the data and the date on which it was checked.

7.1.9 Virus and Data check

The word document held in the ARQ directory on the CD-W shall also contain reference to the anti virus software used to check the CD-W. The CD-W shall be checked for viruses after the data has been written to it and before sending it to Post Office Ltd. The retrieved data is checked by another member of the PSS team prior to despatch.

7.1.10 Despatch

The CD-W shall be sent to the POL Casework Manager by Royal Mail's Special Delivery Service. Appropriate packaging for the CD-W will be used to help protect against damage in transit.

7.2 Prosecution Support

Quotas for all Prosecution Support activities shall be as referenced in the Service Description for the Security Management Service CS/SER/-16.

7.2.1 Check Horizon System Helpdesk Logs

Problems or faults at a Post Office outlet logged with the Horizon System Helpdesk may be required by POL and if so, logs will be examined using the search criteria specified in an ARQ to assess whether the outlet was functioning effectively.

The logs are accessed through the web-based program, TFS. PSS shall use the specified outlet and date range as requested in the ARQ search criteria to search TFS for any calls logged for the outlet in the date range required. The log of calls to the Horizon System

FUJ00122457

Helpdesk details incidents of error, inaccuracy or malfunction pertaining to individual sites, the equipment, services and those individuals concerned.

7.2.2 Analysis of Non-polling reports

Non-polling reports may be required and if so they shall be reviewed for the outlet in question, for all days within the date range specified.

7.2.3 Analysis of Fault logs

If requested, all relevant TFS calls will be reviewed to identify any recorded faults, that might affect the integrity or admissibility of the audit archive from which the ARQs are extracted.

7.2.4 Complete Witness Statement of Fact

PSS will provide witness statements of fact to support data or records retrieved, as requested.

7.2.4.1 Witness Statement of Fact

Any material or otherwise pertinent information shall be recorded and included in the relevant witness statement of fact.

Requirements for witness statements explaining the extraction of audit data from Horizon in response to an ARQ shall, where possible, be completed by the individual from PSS who completed the request.

The statement shall follow the standard format and layout for witness statements of fact provided in evidence. The contents of these statements may vary depending on the specific requirements of the case and the knowledge of the witness providing the statement. However, a standard witness statement of fact has been agreed with POL and is provided at Appendix 2. The standard 'Side B' document which accompanies all witness statements is provided at Appendix 3.

7.2.4.2 Court attendance in support of a Witness Statement of Fact

The author of a witness statement of fact may be required to attend Court in order to bear testimony to the facts.

7.2.5 Provision of Exhibits

Evidence provided in support of prosecutions generally comprise one or more of the following:

- CD-W containing transaction data
- Copies of relevant ARQ request forms

FUJ00122457

- Horizon System Helpdesk logs
- Non-polling reports
- Fault logs

7.2.6 Exhibit Labels

All evidence referred to in the witness statement of fact will require an Exhibit Label. This allows for the evidence to be clearly identified. An example is provided at Appendix 4.

7.2.7 Despatch

Evidence from Horizon System Helpdesk logs, non-polling reports, fault and event logs shall be given an exhibit number and, along with the witness statements of fact, be posted to the Post Office Ltd Casework Manager via Royal Mail's Special Delivery Service. Appropriate packaging of the statements, reports etc. will be used to help protect against damage in transit.

7.3 Prosecution Support Resolution Time Scales

Prosecution Support is not subject to resolution timeframes but The Royal Mail Group Account shall use reasonable endeavours to meet dates notified by Post Office Ltd for the production of this material.

FUJ00122457

8.0 Additional Prosecution Support

There may be occasions when information is requested which exceed that provided by the standard Prosecution Support Service. This shall be dealt with on a case by case basis and in accordance with the Change Control Procedure.

8.1 Audit Record Queries

ARQ retrievals beyond that specified under contract shall be agreed on a case-by-case basis and shall be dealt with in accordance with Change Control Procedures.

8.2 Expert Witness Statement

To offer all the available evidence without it being requested would only serve to flood the courtroom with documentation. For this reason expert in depth analysis and detailed "expert" witness statements (as opposed to witness statements of fact) are rarely required.

It is however conceivable that in certain cases the prosecution may require detailed analysis of a certain issue or function of the system and, given the size and complexity of the Horizon System, it may be necessary to call upon the assistance of an expert in that field. In these cases additional, granular detail about the technical working and integrity of various systems that constitute the Horizon System may be required.

Expert witnesses could comprise anyone within the Royal Mail Group Account or it's approved contractors who could be called upon to provide and testify to this additional evidence.

Expert witnesses could be called upon to provide for example:

- Operational logs and shift hand over documentation to demonstrate consistent operation and availability of the service;
- Secure NT, Dynix and SecurID definitions;
- Details of information flows throughout the system;
- Details of cryptographic key controls and other confidentiality, integrity and availability issues;
- Provision of specific Tivoli and other system security event files;
- Subsequent analysis of this data.

Whilst this type of detail is specifically excluded from the standard evidential requirements included at paragraphs 7.2.1 to 7.2.4, the Royal Mail Group Account will endeavour to provide support of this granular level of evidence on an agreed case by case basis and shall be dealt with in accordance with the Change Control Procedure. Again, The Royal Mail Group

FUJ00122457

Account shall use reasonable endeavours to meet dates notified by Post Office Ltd for the production of this material.

8.3 Court Attendance in support of an Expert Witness Statement

Attendance at Court in support of an expert witness statement shall also be considered on production of an appropriate Change Request. The Royal Mail Group Account's charges for assistance in this respect shall be calculated on the basis of the rates set out in Schedule A12.

FUJ00122457

9.0 Appendices

9.1 Appendix 1

ARQ Blank .doc

9.2 Appendix 2

Standard Witness Statement V6 .doc

9.3 Appendix 3

Witness Statement Standard Side B.doc

9.4 Appendix 4

Exhibit Label.doc

FUJ00122457