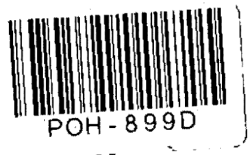
FUJ00058509

ICL PATHWAY INTERNAL AUDIT

BRIEFING NOTE



To : **Miles Blewett, Masons** [GRO]

From : **Jan Holmes, Pathway Audit Manager**

Copy : **Tony Oppenheim, Pathway Finance Director**

Martyn Bennett, Pathway Quality & Risk Director

Date : **28th January 2000**

Subject: **ACCESS TO HORIZON AUDIT DATA BY POCL SECURITY INVESTIGATIONS**

Miles, I've attempted to provide as much information as I think you will need in advance of Thursday's meeting with Martyn and I.

There are a number of attachments with this note :

1. Audit Trail Functional Specification V3.0 dated 1st July 1999
2. Minutes from Audit Panel meeting dated 14th January 1998
3. Minutes from Audit Panel meeting dated 12th February 1998
4. Minutes from Audit Panel meeting dated 14th May 1998
5. Letters from POCL and BA regarding data extractions dated 15th and 16th July 1998
6. Keith Baines letter dated 11th january 2000.

Please note that any handwriting on any of these document was done at the time.

Definitions

The following are key definitions from Schedule A0.

Transaction:

A recorded and auditable instance of business activity, involving service provision or Stock movement across organisational or service boundaries.

Event:

A recorded and auditable instance of business administration activity, such as the registration of a new User, or the production of a Report.

Records:

Full and accurate records relating to the performance of the POCL Services.

Agent:

Any person authorised to operate a franchise post office or sub-post office, including without limitation sub-post masters on a non-franchise contract, and franchisees of post offices or sub post offices.

POCL Data:

Means all data, information, text, drawings, diagrams, images or sounds which are embodied in any electronic or tangible medium, and which are supplied or in respect of which access is granted to the Contractor by POCL pursuant this Codified Agreement, or which the Contractor is required to generate for POCL under this Codified

FUJ00058509

Agreement, but excludes the Service Architecture Design Document and Documentation.

Access to Audit Data

During Acceptance, Audit was dealt with as two separate areas, Operational Audit and the related Audit Trail and Commercial Audit and the related Records.

Each was linked to a specific Requirement, Operational being R699 and Commercial being R697. These terms were coined in the Audit Trail Functional Specification (ATFS Section 1.1.1), a document that all parties were conversant with and which is now a CCD – latest version is 3.0 dated 01/07/99.

The ATFS identifies the roles that have access to audit data and rules surrounding that access (Sections 1.2.2 and 1.2.3). There is no mention in this document of 'POCL Security Investigations', either a role or an organisation.

It acknowledges access at two levels, at the Counter and at the Centre. It states that "all access at the centre is via the Pathway audit function."

Each was 'Accepted' through independent Acceptance Reviews; Operational via Audit Data extractions against pre-prepared Requests For Information, the agreed process; Commercial via an audit of the commercial arrangements by a mixed BA/POCL team resulting in an Audit Report. This was conducted under the auspices of the Joint Working Framework (JWF), itself an accepted interpretation of Schedule A03. The JWF is described in the Horizon System Audit Manual (HSAM).

The Audit data is further demarcated through its retention, Operational Audit Data is retained for 18 months and Commercial Audit Data for 7 years.

The Horizon System Audit Manual (HSAM) and its associated low level procedure provides detailed and explicit arrangements for access to the Operational Audit Data at the Outlet and at the 'Centre' – this is access to data not available at the Outlet. This is a practical implementation of the rules established in the ATFS. HSAM was developed with considerable input from BA/POCL and it was accepted during Acceptance as a definitive document, albeit not a CCD.

The requirements for (Operational) Audit Data Retrieval are defined in a document that was directly contributed to by BA and POCL through written statements of the type, frequency and turnaround time that they expected. Throughout this activity POCL maintained the position that Network Auditors would not require access to data held at the 'Centre'. Access by POCL Investigations was not discussed nor allowed for by either party.

It is understood that during this time POCL Investigations were pursuing their own data retrieval requirements through the Fraud Risk Management System (FRMS), a BA service.

The Quoted Bits of the Contract in Keith Baines' Letter

Clause 801.

801.1 & 2 : This refers to Records but what does Records mean in this context. It talks about 6 years which would exclude the Operational Audit Trail.

801.3 : It talks about "investigations into suspected fraudulent activity or other impropriety by the Contractor or any third party..." but the exclusion of the Operational Data implies that this is financial impropriety in the execution of the contract and not the service. Thus it is targeted at Pathway and not a POCL Agent as defined in Schedule A0.

FUJ00058509

Schedule A03

This is a bit more tricky!

2.1 : Here they have re-defined POCL's Agents as specifically themselves, their external/regulatory auditors (what's the difference?) other agents or successor to any of them. Presumably they could identify POCL Security Investigation Branch as 'POCL' to support their claim.

3.1 : We are required to maintain an 'audit trail' of Transactions (see above) and Events (see above) in strict conformance to Schedule A2 para 4.1.4 (see below) by their definition this equates to the Operational Audit Trail (R699).

4.1 : Talks about access to the Records (see above) and additional stuff. This is a crib from R697 - or the other way round) - and equates to the Commercial Audit Trail as defined in the ATFS accepted by POCL.

The combination of 3.1 and 4.1 implies the full set of audit data, records, call it what you want, has to be available to them!

4.2 : Limits access by POCL Agents to data held by the Contractor in Outlets.

4.3 : Requires us to provide 'reasonable assistance', therefore no set turnaround and frequency requirements established. This to support their needs to supply information for, among other things, judicial purposes. Does this mean prosecutions in which case this is dealt with in R829.

4.5 : Says that upon notification Pathway has to provide access to the audit trail in para 3.1 – taken to be the Operational Audit Trail and the facility to interrogate that trail using reasonable selected criteria.

The rest of it revolves around the carrying out of audits and a fairly general audit process with which we must comply. This is enshrined in the JWF, tested under acceptance of R697, the Commercial Audit Trail.

Statements

1. **In his initial analysis of the problem Warren introduced R894 as, potentially, the basis for their claim. I am unhappy with that as R894 did not form any part of the contractual acceptance that the audit solution went through. Are we not shooting ourselves in the foot by introducing something that has played no previous part in our thinking or actions.**
2. Arguably we already provide ~95% of what they want via the TIP link on a daily basis. Some work would have to be undertaken by us to ensure that we provided the Event information but this may be a 'less cost' option than providing the info via the TMS journal (which is the nub of their current argument).
3. This could service their 'fishing trips' which I believe account for the 'few hundred' queries anticipated by Bob Martin. We would then extract from the audit archive to form the prime evidence for prosecution or dismissal. This approach was discussed with Hilary Stewart (POCL) during the development period and Acceptance.
4. In this scenario we could still meet R829 since they could advise us of the characteristics of data they wanted retained beyond the normal 18month retention period.

FUJ00058509

5. POCL have always maintained a organisational distinction between the Network Auditors, who access the system at the OUTLETS and the Central Auditors who have access to historical audit data at the CENTRE, via Pathway Internal Audit.

6. POCL have always been involved in the development of the Audit Trail Functional Specification, the Audit Data Retrieval Requirements and the Horizon System Audit Manual where this separation has been reflected in the solution currently implemented.

7. The audit solution in its current form has been formally accepted by POCL.

8. Clause 801 is a red herring as it is about financial impropriety by us or our agents, despite their attempted catch-all of 'any third party'. How can we be held responsible for a dodgy PostMaster, operating our system perfectly correctly but defrauding the Post Office as a result!

9. Regardless of the scope of Schedule A03 it appears to limit itself to POCL data held in the OUTLETS. (Actually, if that holds does it not render the remainder of A03 worthless).

10. Throughout 1997, 1998 and 1999 a three way liaison group, known as the Audit Panel, met regularly under the chairmanship of the PDA, to discuss the practical, day to day issues surrounding audit. Minutes were taken after each meeting and circulated to attendees. Copies of the minutes from 14/01/98, 12/02/98 and 14/05/98 are attached. Summary - and I've marked the paper copies – of relevant areas :

Meeting 14th January 1998

i. Dave King (POCL Fraud & Security Group) to discuss with Lee Harris (POCL Internal Audit) appropriate links for security queries and general investigations.

ii. Lee Harris to discuss agreement to use Data Warehouse as basis for investigations and prosecutions with Dave King. (Note that I'm not sure what 'agreement' this is referring to.

iii. Graham King (Pathway Fraud Risk Manager) and Jan Holmes (Pathway Audit Manager) led general discussion on investigations. POCL Regional Security Investigation Managers mentioned. Thrust was information to Pathway from POCL in support of the then Pathway liability for fraud perpetrated through our system.

Meeting 12th February 1998

i. Dave King agreed that Pathway FRM links to POCL should be via FSG – now non-existent. (Point iii. above)

ii. The Lee Harris/Dave King discussions re Data Warehouse as basis for investigations no longer relevant and dropped from meeting. (Point ii. above).

iii. Jan Holmes seeking specific details of audit data retrievals. Note the handwritten comment re 'No! Refer to ATFS'. This is because the ATFS does not allow access of this type for POCL Regional Audit.

iv. Dave King agreed to provide figures to support his comments surrounding Security Event Investigations.

Meeting 14th May 1998

i. Figures to be supplied for Point iv. above deemed to belong elsewhere and dropped from the Panel agenda.

FUJ00058509

Essentially there are no other mentions of audit data requirements for anybody other than POCL Internal Audit.

11. There are two letters which establish POCL's and BA's position with regard to Audit Data retrieval Scenarios. You will note Hilary's comments regarding historical extractions for her regional audit colleagues. I cannot find any evidence that I replied to her request. I do recall conversations with her over a period of time where we discussed the potential for POCL using TIP data for their 'fishing trips' and then coming to me for the true data once they had progressed their investigations to a point of prosecution or dismissal. We never formally agreed that this would be the way to go but the potential was aired. Again though, note that it was her 'regional audit colleagues' and not POCL Security Investigations.

12. In February 1999 Bob Martin (POCL Investigations) provided GPK with Terms of Reference for a paid study vis "To ensure that the work undertaken by Pathway to determine the costs of providing an enquiry service within the Horizon system for POCL investigation staff accords with the requirements laid down by POCL Security & Investigation Executive". The ToRs identified 8 separate requirements, some of which equate to the level of detail currently being requested. This was referred to SDoyle for some initial feedback which he provided in a memo to MHB dated 2/3/99. He also declined to provide an estimate until clearer requirements were presented by POCL. In a letter dated 11/3/99 from Bob Martin to MHB Bob explained his funding problems and agreed to come back to MHB once the position was known. There has been no further correspondence until Bob attempted to meet his information retrieval requirements through Service Management and the rest is history.

This tells me that POCL knew they were exposed as early as February 1999. The earlier discussions during Audit Panel meetings were held with Fraud Risk Management, a separate part of Pathway to Audit. Bob Martin's paid study was sponsored into Pathway by Fraud Risk Management.

Security Standards

4.1.4 The Contractor shall adhere to the relevant parts of POCL's security standards and requirements listed below, and co-operate with POCL to assist POCL in complying with those standards and requirements:

'Social Security IT Security Standards' (reference DITSG\ITSS\0001.04, version 6.3 dated September 1996) to the extent applicable to OBCS and to the POCL Infrastructure Services necessary to deliver OBCS;

'Post Office Counters Information Systems Security Policy' (as provided in Appendix 4-1 of the BA/POCL SSR issued in April 1995); and

'A Code of Practice for Post Office Information Systems Security' (Version 1.5 dated 28/10/94, as provided in Appendix 4-2 of the BA/POCL SSR issued in April 1995).