Document Title:	PATHWAY RISK RESPONSE RISK : PWY 066
Document Type:	Risk Response
Abstract:	This document describes how Pathway is addressing the above risk contained in the Pathway BA/POCL Risk Register. The risk concerns the potential use of dongles to minimise the risk of corruption during multiple PC failures in a post office.
Distribution:	BA/POCL Risk Owners : J Folkes Pathway Quality and Risk Management Director
Document Status:	Issued
Document Predecessor:	None
Associated Documents:	BA/POCL Risk Register, Version 13, 5th January 1996
Author:	Dave Cooke
Approval Authority:	M H Bennett, Director Quality and Risk Management
Signature/Date:	
Comments To:	Dave Cooke

0.1 CONTENT

0.1.1 DOCUMENT HISTORY

Version	Date	Reason
1	17/1/96	Draft

0.1.2 ASSOCIATED DOCUMENTS

Version	Date	Title	Source
13	5/1/96	BA/POCL Risk Register	

0.1.3 ABBREVIATIONS

BA	Benefits Agency
BPS	Benefit Payment Service
PAT	Project Assurance Team
PID	Project Initiation Document
POCL	Post Office Counters Limited
SIS	Strategic Infrastructure Service
SSR	Statement of Service Requirement

1. INTRODUCTION

This paper provides the response to risk PWY066 identified by the POCL Infrastructure Strand meeting. Pathway believe that this response should enable the BA/POCL team to remove this risk from the register.

2. STATEMENT OF THE RISK

Escher have recommended that Riposte requires strong sequence numbering and strong identity to ensure maximum resilience of the message store and to minimise the risk of corruption during cases of multiple failure. They suggested that a dongle providing terminal identity and monotonically increasing sequence numbers would be their preferred solution.

Please advise if Pathway are planning to follow this recommendation, and if not what alternative mechanism will be used to provide the same level of resilience.

3. PATHWAY RESPONSE

During various meetings between POCL, Escher and Pathway a multiple failure scenario in a post office was constructed which, given a particular recovery sequence, could result in a counter PC being recovered to an incomplete state. During these discussions the use of an auxiliary peripheral device - or dongle - was raised which would allow Riposte continually to record the latest sequence number for a PC in another place as well as on the hard disk.

Following a PC failure, this detachable device would then be transferred to a replacement PC to check that the latest recovered sequence number was consistent with the last actual sequence number.

The failure scenario is expected to be extremely rare, based upon ordinary assessment of probabilities and operational experience in Ireland. It requires that all the PCs in a multiple counter post office will be in a failed state together at a particular point in time. This would include the gateway PC whose failure would prevent the latest sequence numbers known by the correspondence server being used to support counter PC recovery.

In this scenario the use of a dongle is one method of identifying an inconsistent recovery although one which does not of itself guarantee the correctness of recovery.

In developing the overall technical and operational solution for BA/POCL, Pathway are mindful of the need to constrain costs wherever reasonable and to ensure that simple, robust operational procedures are followed in extreme failure conditions. In addition Pathway is providing a facility within EPOS to assist the user in transaction recovery. This is required for the failure in a single counter post office, and will also be used when all PCs fail in a multiple counter post office.

Sequence numbers are a key mechanism in ensuring that secure replication occurs between all counter PCs and the correspondence servers, and are fundamental to the automatic recovery process. The Pathway solution is resilient to multiple failures in an outlet and, providing at least one counter PC remains operational, then subsequent recovery of counter PCs will always correctly use their latest sequence numbers and associated transactions. The use of a dongle is not required to effect this.

The Pathway solution for OPS utilises Ethernet hubs so configurations of a broken ring type, where a local are becomes divided into two operating sub-lans are not possible.

In addition, dongles being by their nature transferable pose an operational integrity threat beyond the control of the service provider, should they be transported or moved inadvertently or maliciously.

The correspondence server may always be slightly out of step with an outlet due to normal replication delays, so should one of the failures involve the gateway PC this will not affect the automatic recovery.

From the various failure combinations two general cases in a multiple counter post office are defined where special action is required :-

- A counter PC becomes disconnected from the LAN (e.g. cable failure).

  In this scenario the counter PC will detect that it has become disconnected and Pathway's recommendation is that this PC, unless it is the gateway PC, be taken out of service for benefit payments.

  Pathway understands that in a busy office it may be helpful to allow some business to carry on, but in this situation certain transactions would have to be disabled. These would normally include benefit payments, although in smaller offices this service could continue provided the risk of multiple payments was addressed by physical observation.

  Should this PC subsequently fail, having continued working on a subset of transactions it will be recovered from other PC's to the point when it became disconnected from the LAN. Any transactions carried out while the PC was disconnected from the LAN would be lost. This situation is analogous to the single counter post office failure.

  Knowledge of a difference in sequence numbers between highest recovered and highest actual would not greatly assist the user. The user would know that this situation had occurred, and the key task is to assist the user in recovering any lost transactions and in maintaining the stock unit accounting.

When the PC was recovered from the others in its group the EPOS system would advise the user of the last known transactions(s) and the stock/cash position as known by the system. This would enable the user to recover any transactions for which client vouchers were taken and to reconcile his cash and stock position.

It is for these reasons that Pathway recommends that PCs other than the gateway PC, be taken out of service for benefit payments.

- All PCs in an outlet progressively fail

  Should this situation occur a high priority service operation would be initiated. In order to protect the integrity of the outlet the recovery procedure would require that the gateway PC is restored first from the correspondence server. Other counter PCs would then be progressively restored.

  Recovery will not be permitted to take place exclusively from a PC which has become detached from others in its group and subsequently reconnected, since it will not be aware of the latest sequence numbers used by other PCs.

4. SUMMARY

Pathway believes that the scenario which could produce inconsistent sequence numbers in the Pathway configuration will be very rare and could only occur when all counter PCs in a multiple counter office were failed simultaneously . This failure situation would be handled by Pathway on an exceptional basis and a rigorous recovery strategy will be used to ensure all PCs are logically consistent.

The use of a dongle would not be required to identify that such an event had occurred and could pose operational threats. The important function of assisting the user to identify any lost transactions will be provided as part of the EPOS application.