POL00029278



| | |
|---|---|
| **Document Title:** | Major Incident Report for Network Banking Failures on Monday 5th January 2004 |
| **Document Type:** | Report |
| **Release:** | |
| **Abstract:** | Report covering the partial loss of all on-line services for 30 minutes in the morning of 5/1/2004, followed by total loss of the Network Banking Service for an hour and a half in the afternoon. |
| **Document Status:** | Approved |
| **Originator & Dept:** | Mike Woolgar and Peter Burden - POA Customer Service |
| **Contributors:** | Julie Welsh, Dave Tanner, Colin Johnson,<br>John Samuel (Energis) |
| **Internal Distribution:** | Distribution for draft - as per section 0.2<br>Distribution for Approved version - as above plus Pete Jeram, Liam Foley, Colin Lenton-Smith, Ian Lamb, Richard Brunskill, Ian Morrison, Bill Mitchell |
| **External Distribution:** | Dave Hulbert |

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

| Name | Position | Signature | Date |
|---|---|---|---|
| Martin Riddell | FS POA Service Director | | |
| | | | |
| | | | |
| | | | |

POL00029278



# 0.0 Document Control

## 0.1 Document History

| Version No. | Date | Reason for Issue | Associated CP/PinICL |
|---|---|---|---|
| 0.1 | 15/1/2004 | Initial Draft | |
| 0.2 | 16/1/04 | Second Draft | |
| 0.3 | 16/1/04 | Third Draft | |
| 1.0 | 23/1/04 | Approved version | |

## 0.2 Review Details

| | |
|---|---|
| Review Comments by : | |
| Review Comments to : | |

| Mandatory Review Authority | Name |
|---|---|
| *See Review Role Matrix in PA/PRO/010* | |
| Fujitsu Services Post Office Account | Dave Tanner |
| Fujitsu Services Post Office Account | Colin Johnson |
| Fujitsu Services Post Office Account | Martin Riddell* |
| Fujitsu Services Post Office Account | Julie Welsh |
| Fujitsu Services Post Office Account | Tony Wicks |
| Fujitsu Services Post Office Account | Mike Stewart |
| Fujitsu Services Post Office Account | Dave Law |
| Optional Review / Issued for Information | |
| | |
| | |

( * ) = Reviewers that returned comments

## 0.3 Associated Documents

| Reference | Version | Date | Title | Source |
|---|---|---|---|---|
| | | | | |
| | | | | |

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

POL00029278



## 0.4 Abbreviations/Definitions

| Abbreviation | Definition |
|---|---|
| BCM | Business Continuity Manager |
| CFM3 | Core Services Networks |
| DM | Duty Manager |
| FAD | Financial Accounts Division (Post Office) |
| FRIACO | Fixed Rate Internet Access Call Organisation |
| HSH | Horizon System Helpdesk |
| HSRP | Hot Standby Routing Protocol |
| ISDN | Integrated Services Digital Network |
| IVR | Interactive Voice Response |
| NB | Network Banking |
| NBE | Network Banking Engine |
| OCP | Operational Change Process |
| PIR | Post Incident Review |
| PM | Problem Manager |
| PMDB | Problem Management Database |
| PO | Post Office |
| POA | Post Office Account |
| POL | Post Office Limited |
| SMC | Systems Management Centre |
| TSD | Technical Services Desk |

## 0.5 Changes in this Version

| Version | Changes |
|---|---|
| 0.1 | This is the first draft |
| 0.2 | Updated following comments |
| 0.3 | Updated following comments |
| 1.0 | Procedure review frequency has been added. Also, actions due as specified |

POL00029278



| | |
|---|---|
| | in Section 7 have been updated. |

## 0.6 Changes Expected

| Changes |
|---|
| |

POL00029278



# 0.7 Table of Contents

POL00029278



# 1.0 Introduction

This document reports on the issues that arose from two major incidents affecting the Network Banking Service that occurred on 5th January 2004.

This report covers:

- How the problems came to light
- The impact on the branch service
- The investigation
- The resolution
- The root cause
- Actions and recommendations to prevent recurrence

# 2.0 Scope

The scope of this report is two major incidents that occurred on Monday January 5th The first affected all on-line transactions for some 30 minutes for a subset of the branch estate. The second caused the loss of the Network Banking Service for an hour and a half to the full estate.

# 3.0 Management Summary

The **first incident** caused 70 Post Offices to log calls stating that the Offline Indicator had appeared on the screen. The advice from the HSH was to log off and log on again and this resolved the Post Masters' issue. The first call was logged at 11.45 and the problem was cleared by 12.05. In that timeframe a further 400 calls were abandoned. The problem was caused as a result of a software problem that Energis encountered while they were undertaking maintenance work. The problem was overcome by Energis and this, together with the availability of alternative routing, meant that the impact was minimised.

Correct escalation routes - including to POL - were followed.

The procedure agreed following the Off Line Indicator fails on 7th and 25th November was invoked. This was to get a sample of FAD ISDN numbers to Energis within minutes. This worked very successfully and ensured confirmation that the failures experienced by the Post Offices which had logged calls were indeed amongst those which Energis would expect to see affected by the problem that they had encountered.

The **second incident** in the afternoon of 5th January had the effect of losing the Network Banking Service to the full estate for an hour and a half. It was caused by a failure in a Fujitsu Services encryption router at IBM Warwick.

POL00029278



Upon the failure of the primary encryption router, fail-over to the secondary encryption router should occur automatically. This did not happen.

Attempts by the Core Services Networks team to enlist IBM's assistance in resolving the issue were delayed because the wrong support route was invoked.

Service was resumed following a software reboot of the encryption router.

Some symptom similarities with the incident in the morning and the "relatively" low rate of calls to the HSH - some 80 calls in a one-hour window (with, again, some 400 abandoned) - also contributed to unsatisfactory handling of this incident, including an unacceptable delay in briefing POL.

Corrective actions are identified in a later Section but the primary ones are as follows

- the Core Services Network team procedure for requesting IBM support has been updated. It should be noted that all procedures are reviewed on an annual basis, with urgent changes being made as required.
- a change to the Hot Standby Routing Protocol on the encryption routers, that will cater for the type of failure that occurred on 5th January and ensure fail-over, is planned for implementation over the weekend of 17/18 January
- a manual procedure to effect failover has been put in place. This can be invoked should automatic failover not be successful.
- plans for enhancements to Business Continuity Testing in this area will be reviewed, with initial proposals by 30th January. This will be followed by a wider review across other areas.
- the necessity for promptly advising POL of such incidents has been re-inforced to POA service managers
- Energis to propose revised criteria for advising Fujitsu Services of operational change activity and how the likelihood of a change being service-affecting is assessed

# 4.0 Description of the fault and service failure

## 4.1 Symptoms and Business Impact

### 4.1.1 Symptoms as seen by Branches

In the **first incident**, from 11.45 for a period of some 20 minutes , 70 Post Masters called the HSH as they were unable to perform on-line transactions on the Horizon equipment because the Offline Indicator was present. The advice from the HSH was to log off and log on again and this resolved the Post Masters' problem. There would nevertheless have been some impact on customers who were visiting Branches.

POL00029278



In the **second incident** no Post Master, from around 14.50, would have been able to perform any Network Banking transactions on the Horizon system, for about an hour and a half. This would have had a corresponding impact upon customers who were visiting Branches.

No Network Banking transactions were processed through the NBE and onto the relevant Banks.

4.1.2 Symptoms as seen by Fujitsu Services

On the **first incident**, HSH received 70 calls by 12.00 stating Off Line Indicator with a further 400 calls being abandoned. SMC had seen Fatal Events on Warwick Encryption Router 2. Energis saw a drop of FRIACO ports (a maximum of 3000) and then saw them restore 10 minutes later.

On the **second incident**, SMC saw Fatal Events on Warwick Encryption Router 1. This was followed by the HSH receiving about 80 calls within an hour - with a further 400 abandoned. No issues were visible to Energis.

## 4.2 Detailed explanation of the incident

The **first incident** was caused by maintenance work that Energis were undertaking to tidy tables on a network router at Watford. This was expected to be routine work that should not affect any live service. Hence none of their customers, including Fujitsu Services, should have been affected. In undertaking this work, however, Energis encountered a software problem and then had to revert the router to its previous state. The dial plan between Fujitsu Services and Energis provides for alternative routing, which, along with the swift rectification by Energis, explains why affected Branches were able to successfully retry their transactions.

The software problem referred to above is a Cisco problem. Energis have advised that in terms of service impact it is safe to refrain from tidying the relevant network tables until further information on the problem is obtained.

The **second incident** was attributable to a failure on Encryption Router 1 at Warwick and the subsequent failure to fail-over to Encryption Router 2.

The delay in getting Encryption Router 1 back up and running was primarily due to the Fujitsu Services Core Services Network Team not using the correct procedure for enlisting IBM's assistance. Essentially the team contacted some IBM staff directly rather than using the correct route which is via the TSD. It was unfortunate that the IBM staff who were contacted initially were not able to assist, but it is recognised that the wrong procedure was used by Fujitsu Services. By the time that the appropriate IBM staff were involved the router had rebooted itself and the service was thus restored.

POL00029278



The core dump from the failing router has been examined by Cisco. Their response has been that from the evidence available they are not able to determine any cause for the encryption router failure. Neither does the evidence assist as to the reboot.

The failure to fail-over to Encryption Router 2 is now understood (following the investigative work undertaken over the weekend of 10/11 January) and an enhancement to the Hot Standby Routing Protocol is planned that will deal with the situation that occurred on the afternoon of 5th January. This situation being that Encryption Router 1 had lost its encryption tunnels to the Horizon Data Centre but in other respects was functional.

It is noted that Business Continuity testing across the link from the Horizon data centres to Warwick has to date been effected by generating a hard fault (removing the cable) at the data centre end. The incident in the afternoon of 5th January has shown that some changes to future Business Continuity testing are required and there is a corrective action in a later section to cover this.

# 5.0 Incident Management

| *Date & time* | *Avoidance, mitigation and resolution activities* | *Communication and escalation activities* | *Business Impact* |
|---|---|---|---|
| | ***INCIDENT 1*** | | |
| *05/01/04 ( all on 5/1/04)*<br>*11.34* | *SMC saw fatal events on Warwick encryption router.* | | |
| *11.47* | *SMC raised a call and passed to CFM3 for investigation*<br>*E-0401050573*<br>*E-0401050601.* | *SMC paged POA DM who immediately appointed POA PM who informed acting POA BCM who informed POL BCM and POA Operations Manager.* | *Extent unknown at this time.* |
| *11.48* | *Energis informed POA Network Service Manager of a Router fault at Watford and that the service may be affected.* | . | . |
| *11.50* | *POA DM continually updating POA PM that several PO's had placed calls stating Off Line Indicator showing* | *POA Problem Mgr updating POA BCM* | |
| *12.00* | *POA DM stated that 70 PO's had logged calls and another 400 had been abandoned. The HSH had told the PO's to log off and then log on again. This appeared to* | | *HSH had received 70 calls from Post Office branches at this time.* |

POL00029278



| | | | |
|---|---|---|---|
| | *clear the fault.* | | |
| *12.05* | *TSD raised a call to state that possibly up to 25% of the estate could be affected.*<br>*E-0401050624* | *POA DM informed and then POA PM updated.* | |
| *12.05* | *Energis called Networks Service Mgr to state fault had been cleared and also that resilience kicked in successfully* | *POA PM advised Energis that a sample of FAD ISDN Nos' would be sent across for investigation* | |
| *12.10* | *"High Call Volumes" IVR message applied* | | |
| *12.10* | *SMC state problem completely resolved to POA DM* | *POA DM informed POA PM of situation ,and POA BCM informed.* | *HSH had by this time received 400 abandoned calls from Post Office branches. However the service was now up and running.* |
| *12.20* | | *POA BCM advised POL BCM of situation* | |
| *12.30* | *CFM3 forwarded Sample of ISDN No's to Energis for investigation.* | | |
| *12.51* | *POA PM raises problemPM000447 for incident on PMDB, in order to progress fault diagnosis and ongoing investigations, recommendations and resolutions* | | |
| *13.30* | *Energis confirm that symptoms from ISDN Nos are as per the problems they have evidence of.* | | |
| | | | |
| | ***INCIDENT 2*** | | |
| *15.02* | *Call 601 updated by SMC to say they have seen fatal event on Warwick Encryption Router. This was confirmed by CFM3 who had seen an encryption failure. Call is subsequently upgraded from B to A, following earlier downgrade* | *TSD made aware. POA DM made aware. POA PM made aware and escalated to POA BCM.POA PM also informs Energis that FAD ISDN No. samples will be coming across and asks if Energis experiencing any similar issues to the morning failure.* | |
| *15.13* | *SSC contact TSD ref seeing NBE engine down*<br>*Call 624 updated, but also confirm no call has been received from IBM* | *CFM3 attempt to contact IBM to reboot router* | |
| *15.14* | *SMC give sample of FAD No's to* | | |

POL00029278



| | | | |
|---|---|---|---|
| | *CFM4 in order to send ISDN NO's to Energis for investigation.* | | |
| *15.30* | *HSH have received calls from 30 Post Offices* | | *30 Post Offices experiencing either Loss of Network Banking Service or Off Line Indicator showing.* |
| *15.40* | *IBM state that the connection to Fujitsu appears to be OK, that there are no outstanding issues in their domain, but that the incremental transaction counter had stopped* | | |
| *15.42* | *CFM3 provide ISDN No's to Energis for investigation* | | |
| *15.45* | | *POL Problem Manager calls POA BCM and update is provided* | |
| *15.45* | *HSH confirm that 50 Post Offices are now affected* | *Energis confirm to POA PM that nothing untoward with ISDN No's provided.*<br>*POA DM made aware by HSH and POA PM* | *Total of 50 POs' now affected and have no Network Banking* |
| *16.00* | *HSH confirm to POA DM that a total of 80 calls have now been logged* | *POA DM updated POA PM who updated POA BCM* | *Total of 80 Post Offices have logged calls that they have no NB Service* |
| *16.10* | *POA PM escalates to Mgr of CFM3* | *Mgr of CFM3 investiagting* | |
| *16.15* | *TSD chasing IBM for contact name to reboot server* | | |
| *16.20* | | | *HSH had by this time received 123 calls from Post Office branches (and a further 400 calls had been abandoned)* |
| *16.30* | *CFM3 state router has come back up at 16.24 and service starting to come back up after producing dumps* | *SMC, TSD,POA DM, POA PM,POABCM, POA OPS MGR all informed* | |
| *16.35* | *Energis confirm to POA PM that all ISDN No's for sample FADS tested ok earlier.* | | |
| *16.40* | *CFM3 sending diagnostic dumps to NTL for investigation.* | | |
| *16.57* | *IBM confirm to CFM3 that there* | | |

POL00029278



| | | | |
|---|---|---|---|
| | *was no hardware reboot performed* | | |
| *16.58* | *HSH having spoken to PM's affected, confirm that all is running OK* | | *Confirmation that NB is back up and running at the affected PO's* |
| *17.00* | | *POA BCM updates POL BCM* | |
| *17.00* | *POA PM raises problemPM000448 for incident on PMDB, in order to progress fault diagnosis and ongoing investigations, recommendations and resolutions* | | |
| *17.00* | *IVR message is taken off* | | |
| *17.09* | *SMC downgrade call to B priority* | | |
| | | | |

It should be noted that, additionally, senior management in POA and, onwards, senior management in POL were advised of these issues during the day.

# 6.0 Problem Management

The **first incident** was well managed and appropriate procedures were followed. The instigation of the timely provision of the ISDN numbers for affected Branches to Energis for investigation was successfully used for the first time. There was timely escalation within POA and into POL. Energis rectified the problem quickly. Problem (PM0000447) has been logged for the incident.

Energis did not consider that it was necessary to advise Fujitsu Services via an OCP of their intention to carry out the tidying of the network tables. This was because it was not expected to be service-affecting. As a result of this incident Energis have been asked to review the criteria for determining the need for an OCP and how the likelihood of a change being service-affecting is assessed. Their proposals are expected in a week's time.

The **second incident** (logged as PM0000448) was not well managed. In addition to the technical failure that prevented automatic failover to Encryption Router 2, the use of incorrect escalation routes into IBM delayed resolution. The delay in formally advising POL of the problem was unacceptable. Fujitsu Services staff were endeavouring to fully understand all aspects of the problem so that a complete picture could be given to POL, but got the balance wrong between that and the necessity for early advice to POL. Corrective actions in these areas have been identified and are recorded in the next section.

The fact that there were some similarities between the symptoms of the two incidents undoubtedly clouded the issue.

A Post Incident Review was held the following morning between POL, POA and IBM and actions were identified. For completeness the following section encompasses those actions.

POL00029278



Further investigative work on the failure of the fail-over process was carried out on 11th January. The result of this work has contributed to some of the corrective actions in the following section.

# 7.0 Corrective Actions

| *Incident/problem Issue* | *Action to be taken* | *By Whom* | *By When* | *Progress made* |
|---|---|---|---|---|
| ***Incident One***<br>*Failure of Energis to advise Fujitsu Services of operational change activity* | *Energis to propose revised criteria for advising Fujitsu Services of operational change activity and how the likelihood of a change being service-affecting is assessed* | *Energis Service Manager* | *23/1/04* | *[23/1/04 – initial response provided by Energis but further discussions being held]* |
| | | | | |
| ***Incident Two***<br>*Following PIR, that was attended by all relevant POA persons and chaired by POL BCM., the following actions were agreed.* | 1. *POA to confirm whether or not encryption routers are run on primary/secondary basis or load sharing* | *Dave Tanner* | *10/1/04* | *Completed. Run on primary/secondary* |
| | 2. *POA to obtain report from NTL/Cisco as to why encryption failed.* | *Colin Johnson* | *10/1/04* | *Cisco unable to determine the cause from the evidence* |
| | 3. *POA to explain why transactions didn't switch across to the resilient router* | *Colin Johnson* | *13/1/04* | *Following testing it was confirmed that the encryption within the router had failed, rather than the router itself. The testing on 11th Jan showed that by changing the Hot Standby Routing Protocol (HSRP) the problem could be overcome* |

POL00029278



| | | | | |
|---|---|---|---|---|
| | *4.POA to confirm whether the router restoration of service was a software forced reload*<br>*5.CFM3 Operational procedure to be updated in line with OLA for this service*<br>*6.POA to review ongoing BC Test, to create a 'dirtier test' at a much lower partial level, rather than a solid fail.* | *Colin Johnson*<br>*Colin Johnson*<br>*Tony Wicks* | *8/1/04*<br>*8/1/04*<br>*30/1/04* | *Confirmed as a software reload*<br>*Confirmed as updated* |
| *Failure to fail-over automatically* | *HSRP to be enhanced* | *Dave Tanner* | *17/18 Jan* | *[23/1/04 – Completed on 18/1/04]* |
| | *Procedure in place to allow manual failover* | *Colin Johnson* | | *Complete* |
| *Underlying cause of encryption router failure not understood* | *If failure occurs again (and providing the service is being provided successfully through the secondary router) take additional diagnostics* | *Colin Johnson* | *At time of next failure* | |
| *Failure to promptly advise POL* | *Reinforce the necessity for promptly advising POL of problems (even if they are not well understood at the time)* | *Dave Law* | | *Complete* |
| | | | | |

POL00029278