



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

MAJOR INCIDENT REPORT – Fujitsu Network Issue 19 10 2020 & 21 10 2020

INCIDENT DETAILS		
Organisation Managing the Major Incident	Customer / Account Name / Service Line	Name of the Major Incident Manager
Fujitsu Post Office Account, Fujitsu NOC MIM Team	Post Office Ltd.	Matthew Hatch
Executive Summary	<p>On Monday, 19th of October, Fujitsu observed an Internet connectivity issue, affecting the traffic since 16:17. The issue was affecting all Fujitsu POA services using the Internet. Fujitsu NOC MIM Team investigated the issue. Restoration of affected services started at approx. 17:30. The HSI (High Speed Internet) router issue was confirmed to be the cause of a loss of Fujitsu VPN, UMI and corporate Internet access. TCY02'S interfaces shut down for an unknown reason, in addition a commissioning error with CenturyLink meant that resilient routes were not available, resulting in the loss of internet connectivity for some customers. This was diagnosed as an error on the router by Juniper, which would be fixed by a planned restart.</p> <p>A recurrence of the router failure occurred at 11:51 BST on Wednesday, 21st of October. It affected the same services as on Monday. Fujitsu NOC MIM Team investigated the router on site and failed over the traffic, which restored the connection at approx. 12:43. All affected services started to recover at the same time. The team followed the recommended fix supplied by Juniper and identified that the TCY02 chassis hardware required a replacement.</p> <p>The hardware was replaced at 23:30 BST on the 21st October and was confirmed at 1:10 BST on the 22nd October the router was restored and health checks performed to ensure all services were green.</p> <p>The firmware upgrades and testing on the Fujitsu High Speed Internet platform have been successfully completed on the 10th and 12th of November.</p>	
Incident Summary	<p>On Monday, 19th of October since approx. 16:20, Fujitsu observed a network connectivity issue. As a result, the entire Internet traffic was affected which resulted in a loss of some POL services, which use Fujitsu Internet. Fujitsu POA support and service teams also lost access to the secure Fujitsu VPN (remote access) as a direct result.</p> <p>For the detailed impact of the incident, please refer to Services Impacted and Overview of Service Impact 19.10.2020 sections of this report.</p> <p>Fujitsu POA raised multiple high priority incidents for the affected services</p>	

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

from 16:28. For details of raised incidents, please refer to the Incident Timeline. Investigation with POA technical resources was initiated via bridge call at approx. 16:50, but with difficulties as most Fujitsu users are working from home due to COVID-19 and were affected by no access to the VPN due to the network issue.

During the Fujitsu POA bridge call, it was confirmed with POA Networks Team, that we were facing a major network connectivity issue and suspected onward Internet connectivity traffic has not failed over. Acknowledged that the PODG file transfer is also impacted – POA UNIX Team started to investigate this.

During the POA internal tech bridge call, it was confirmed that Banking, Card Payments, EPOSS, Self-Service Kiosk service remain unaffected. Some services failed over as expected.

At approx. 17:30, the POA users observed that the connection began to be restored and affected services started to recover. Fujitsu were able to resume the uploading of the PODG files at 17:31 following a manual intervention by technical support.

At 17:37, Fujitsu Core Network and NOC ISP&DSL Teams confirmed to Fujitsu POA that at 16:17, the HSI router in Fujitsu TCY02 location suffered an event causing it to stop responding, which affected multiple Fujitsu customers. Fujitsu POA were informed that Fujitsu NOC Major Incident Management Team is managing and investigating the issue since observing the events on the router.

POA monitoring teams confirmed Track & Trace was the last of the services to recover; this went green in HORIce (Fujitsu Monitoring Tool) at 19:20. This was owing to a major incident in Royal Mail Group domain related to the business interface gateway that started at approx. 16:00 and was confirmed as not related to the Fujitsu Network Incident.

A recurrence of the router failure occurred at 11:51 BST on Wednesday, 21st of October. It affected the same services as on Monday. Please see details in Overview of Service Impact 21.10.2020 section of this document. Fujitsu NOC MIM Team investigated the router on site and failed over the traffic, which restored the connection at approx. 12:43. All affected services started to recover at the same time.

The team followed the recommended fix supplied by Juniper and identified that the TCY02 chassis hardware required a replacement.

The hardware was replaced at 23:30 BST on the 21st October and was confirmed at 1:10 BST on the 22nd October the router was restored and health checks performed to ensure all services were green.

The following actions were taken for resolution:

1. Correct the commissioning error with the CenturyLink connection
2. Source replacement Hardware for failing component (router chassis)



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

	<p>3. Install replacement chassis and re-establish internet connections</p> <p>All the above actions were completed by 01:23 BST on 22nd October.</p> <p>The firmware upgrades and testing on the Fujitsu High Speed Internet platform have been successfully completed on the 10th and 12th of November.</p>
<p>Services Impacted</p>	<p>Generic FCN Internet access:</p> <ul style="list-style-type: none"> • DXI Internet access • Bank of Ireland (PODG) • Fujitsu VPN access • British Gas/Payzone • Smart card • Smart Meter • Drop & Go transactions • Ingenico (Card transactions unaffected) • GWS <ul style="list-style-type: none"> ○ DVLA, ○ FMCC / FMCV ○ Health Lottery ○ HPBB ○ National Express • CGI • BWS <ul style="list-style-type: none"> ○ Postal Guaranteed Delivery Date service (PGDD) ○ Post Office Card Account service (PCAI) ○ Bank Account Checker (BKAC) • PODG • CapitalOne • CDP transactions • HORIce monitoring tool access
<p>Affected Configuration Items (e.g. site, no. of affected configuration items)</p>	<p>HSI router in Fujitsu TCY02</p>

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

Analysis of Problem	<p>2 problems :</p> <ul style="list-style-type: none">- A commissioning error with CenturyLink meant that resilient routes were not available, resulting in the loss of internet connectivity for some customers.- A hardware issue requiring the chassis to be replaced on TCY02.
Root Cause Analysis	<p>The HSI router in Fujitsu TCY02 suffered an event causing it to stop responding, which resulted in a loss of Fujitsu VPN, UMI and corporate Internet access.</p> <p>Resilience is dependent on both CenturyLink and Cogent accepting all Fujitsu's public prefixes. The investigation identified that due to a commissioning/configuration error, some of Fujitsu's public prefixes were not being accepted by CenturyLink.</p> <p>The result of this was that routes that should have been available via CenturyLink to and from the internet were not.</p> <p>The net result of this was that when the interfaces on TCY02 shut down, customers who had a dependency on the subset of routes only available via TCY02 lost Internet connectivity.</p> <p>A hardware fault on TCY02 router chassis requiring a replacement.</p>
Corrective Actions	<p>The TCY02 router's interfaces were restored without intervention and normal functionality resumed on Monday, 19th of October at 17:30.</p> <p>POA UNIX removed the lockfiles on the PODG manually to allow the file transfers, rather than waiting for the automated process to run.</p> <p>Fujitsu NOC MIM Team expedited the planned changes and failed over the traffic to the resilient path, which restored the connection on Wednesday, 21st of October starting from 12:43.</p> <p>The following actions were completed on the 21st October to restore and resolve the root cause.</p> <ul style="list-style-type: none">- Correct the commissioning error with the CenturyLink connection- Source replacement Hardware for failing component (router chassis)- Install replacement chassis and re-establish internet connections <p>All the above actions were completed by 01:23 on 22nd October.</p> <p>The firmware upgrades and testing on the Fujitsu High Speed Internet platform have been successfully completed on the 10th and 12th of November.</p>

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

Start - End Date Of Incident	Time of Service Outage	Time Service Restored
19.10.2020 – 16:17-17:30	19.10.2020 - 1 hr 13 min	19.10.2020 – 17:30
21.10.2020 – 11:51-12:43	21.10.2020 – 52 min	21.10.2020 – 12:43

RELATED REFERENCES		
Master Incident	Problem Record	No of Linked Incidents
19.10.2020 - INC6469861 21.10.2020 - INC6485885	PRB0048676	19.10.2020 – 12 21.10.2020 – 4
Previous Occurrence	MTTR	Action required to Close
N/A	N/A	Completion of the MIR Actions
Complaints & Alerts Reference Number(s)	ICT Continuity Plan Reference	Change Record Number
N/A	N/A	N/A

TEAM MEMBER DETAILS	
Role	Team Members
Service Line Lead(s)	Sonia Hussain – POA Head of Online Services
Major Incident Manager - Mandatory	Matthew Hatch, Rajaramana Ravula
Resolver - Mandatory	Fujitsu NOC MIM Team

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

<i>Problem Manager – Case by Case basis</i>	Matthew Hatch
<i>Service Delivery Manager – Case by Case basis</i>	Steve Bansal – Senior Service Delivery Manager
<i>Others – Case by Case basis</i>	Piotr Nagajek

INCIDENT TIMELINE		
Date	Time	Activity
19.10.2020	16:17	The HSI router in Fujitsu TCY02 suffered an event causing it to stop responding where POA is affected
	16:17	Fujitsu POA lost access to the VPN and all the Internet traffic was impacted which result in loss of some POL services which use FJ Internet
	16:23	Fujitsu NOC ISP&DSL Team raised a P1 incident INC6469650 for <i>Loss of Fujitsu VPN</i>
	16:28	Fujitsu POA raised a P1 incident INC6469656 for GWS errors for the National Express service
	16:29	Fujitsu NOC ISP&DSL assessed initial impact - Fujitsu staff working remotely have lost VPN access, staff in the office have lost all internet connectivity. The issue was affecting multiple accounts
	16:32	Fujitsu POA raised a P1 incident INC6469675 for the CDP Interface down
	16:39	Fujitsu POA raised a P1 incident INC6469708 for load balancers issue - <i>associate services with pi11nlb202 and pi11nlb201 are inaccessible</i>
	16:50	POA DM Team started an internal bridge call and getting hold of the technical resources
	17:00	Fujitsu POA investigation with technical resources continued with difficulties as most users are working from home due to COVID-19 and are affected by the VPN issue.
	17:08	Fujitsu POA raised incident INC6469806 for connection issues affecting Postal Guaranteed Delivery Date service (PGDD), Post Office Card Account service (PCAI) and Bank Account Checker (BKAC) service.

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

17:11	Fujitsu POA raised a P3 incident INC6469817 for Branch Access and Collect and return showing critical on HORIce
17:12	Fujitsu POA investigation continued, discussed with POA Networks Team possible network connectivity issue and suspected onward Internet connectivity traffic has not failed over. Acknowledged that the PODG file transfer is also impacted – UNIX Team investigating
17:14	Fujitsu POA raised a P3 incident INC6469826 for Track and trace Showing Critical in HORIce
17:15-17:30	Fujitsu POA investigation with technical resources continued. Fujitsu POA SMC tried reaching Fujitsu NOC ISP&DSL team to get the details, but all NOC resources were engaged in the MIM bridge, trying to resolve the issue
17:17	Fujitsu POA OOH Duty Manager Rajaramana Ravula joined the POA internal bridge call
17:19	Following a manual removal of lockfiles by the UNIX Team, PODG file transfer commenced
17:23	Fujitsu POA SMC raised a master incident for multiple services affected by the network issue – P1 INC6469847
17:32	Fujitsu POA SSC support confirmed VPN access restored
17:33	Fujitsu POA logged incident INC0296097 with POL IT DSD for Internet Traffic Usage (GWS, CDP & HBS services affected)
17:37	POA OOH DM reached NOC resource who informed Fujitsu POA that NOC MIM is still investigating the network issue under Fujitsu NOC major incident INC6469650, however, connectivity is recovering
17:42	On the POA bridge call, it was confirmed that no Card or Banking transactions were affected
17:49	POA SMC confirmed Branch Access and Collect and Returns turned to Green but still, Track & Trace is showing critical
17:58	Fujitsu POA SSC resource confirmed the Track & Trace alerts were occurring BEFORE the network incident. The first alert was observed at 14:29:50. Agreed this need to be investigated separately
18:05	Update from Fujitsu NOC MIM: <i>The issue has now been mitigated and services should now be restored. Bridge call is going on with technical to understand the cause, further updates will be supplied by the MIM team and RFO will be provided by MIM team</i>
18:12	POA SMC informed the Track & Trace alerting amber in HORIce
18:15	Update from Fujitsu NOC Operations Manager: <i>UK - Live Services - P1 - INC6469650 x2 18:00 BST. Loss of Fujitsu VPN, UMI and corporate internet access. Confirmation has been received that services are restoring and customers are able to access external websites. Further investigations into the root cause are ongoing by the FJ Networks team. Next update when more information is available</i>

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

	18:28	POA SSC resource confirmed regarding Track & Trace issue: <i>Track & Trace reporting is near real time - no impact on counter, the messages are queued and sent to Royal Mail / Parcel Force. So if people check the barcodes - would be delayed. The TT barcodes will be processed eventually</i>
	19:13	POA Unix confirmed that BIG (PODG) issue was sorted around 19:00. Related TfSNow incident: INC6470271. Summary of the issue: <i>After the network problems in the afternoon, we had issues with the BAP_FILE_BIG PODG route. The route was running very slowly with a single file taking 20-30 mins to transfer and be renamed. This seemed to recover at approx. 19:00 with the backlog of files all transferred at that point. We believe this was an issue at the BIG end</i>
	19:19	POA SMC confirmed Track & Trace returned to green in HORIce
	19:50	Update from NOC Ops Manager: <i>HSI router at TCY02 had an event issue at router 16:17 causing it to stop responding and caused a loss of service. When the event occurred, some customer traffic rerouted via LD6 link instead but not all services rerouted correctly. Services began to restore at 17:29 without intervention from the Fujitsu third line engineers. Investigations are ongoing with Fujitsu third line engineers and hardware supplier Juniper to understand the cause of the outage. Juniper case has been logged and they have been provided with the event logs, all technical information. The NOC will perform additional monitoring on the HSI routers and escalate any potential issues immediately to the third line engineers.</i>
	22:00	NOC update: <i>AMCS third line support have confirmed that the case with 3rd party Juniper has been accepted as a Severity 1. Juniper have performed initial investigation and requested additional information from the device, which is being supplied by AMCS third line support. Extended monitoring is now in place and will continue overnight with AMCS third line support being contacted immediately any performance issues are detected and a restart of the TCY02 router will be undertaken. Further logs files would also be collected at this point to assist with Juniper investigations. Further hourly status updates will be provided by AMCS monitoring team.</i>
20.10.2020	09:20	NOC update: <i>UK – AMCS - P1 - INC6469650 x5 09:10 BST – Services have been stable all night, Fujitsu are actively working with vendor to understand root cause. Vendor has recommended restarting some services to aid diagnostics (Daemon restart) which is being discussed – likely time 0100 Wednesday morning (this will be confirmed)</i> <i>There are Indications of a hardware issue but more to be done to confirm or otherwise hence the further diagnostics that are required from the restart. Fujitsu continue to work with juniper to understand the root cause and develop an action plan</i> <i>Full active monitoring continues, next update when more information available.</i>
21.10.2020	11:51	A recurrence of the HSI router failure occurred
	11:54	Fujitsu NOC MIM Team informed: <i>Loss of Corp VPN affecting user's in the NOC - contacting MIM and escalating to ISP/DSL team</i>
	12:00	Fujitsu POA SMC raised a P1 incident INC6485885 for CDP critical alerts
	12:00	Fujitsu POA Service Management initiated an internal bridge call

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

12:06	Fujitsu POA raised a P1 incident INC6485949 for Health Lottery GWS critical errors
12:06-12:20	POA Tech bridge call continued. Impact initially assessed, confirmed that monitoring teams in India did not lose access to monitoring tools and were raising incidents
12:13	POA SMC raised a P1 incident INC6486044 for Branch Access and Collect & Return monitors showing critical in HORIce monitoring tool
12:20	POA MAC raised a P1 incident INC6486129, which was bonded with POL IT DSD incident INC0296694
12:28	Fujitsu NOC MIM Team confirmed engineers performing device troubleshooting on site
12:43	On the POA tech bridge call a restoration of VPN access and other services was observed
12:57	POA Infrastructure Manager confirmed with Fujitsu NOC MIM Team that the traffic was failed over to the secondary device and all services were recovered
13:00	Enhanced monitoring by Fujitsu POA was in place
13:05	Fujitsu POA confirmed that First Rate successfully logged into the PODG and pulled the files. Automated transfer of other PODG files clearing the backlog was ongoing
13:40	Fujitsu NOC MIM Team confirmed that a technical bridge call is underway with Networks teams and the vendor in order to restore the primary device interfaces

List of all incidents related to the issue raised by Fujitsu POA on 19.10.2020:

Number	Opened	Short description	Parent Incident
INC6470271	19.10.2020 16:28	PODG route issues on BAP_FILE_BIG	INC6469861
INC6470193	19.10.2020 16:32	Spectrum AlarmNotifier (Check Spectrum Console) : Mon 19 Oct, 2020 - 17:11:07	INC6469861
INC6470133	19.10.2020 16:39	SYSMGT_LOG_AKS_HIH_BAL_ERROR_ID0003 WoodSN15243	INC6469861
INC6469973	19.10.2020 17:08	Observed Multiple PODG Alerts	INC6469861
INC6469847	19.10.2020 17:11	VPN Issues - ITGI1084969	INC6469861
INC6469826	19.10.2020 17:14	Track and trace Showing Critical in HORIce	INC6469861
INC6469841	19.10.2020 17:21	INC0296048 - Unable to perform Drop and Go transactions in all branches	INC6469861
INC6469817	19.10.2020 17:23	Branch Access and Collect and return showing critical on HORIce	INC6469861

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

INC6469806	19.10.2020 17:46	syslog.TCOMLoadBalancer TCOM_MONSERV:MONID:PCAI.SERVICE MONSEV:B DIAG 559 19	INC6469861
INC6469708	19.10.2020 18:11	IRRELEVANT LIVE Service - NEOPOST-L4LB - State Changed	INC6469861
INC6469675	19.10.2020 18:19	ALERTID-4005-00000-0] CDP Interface is down- @@	INC6469861
INC6469656	19.10.2020 18:43	MASTER INTERNAL Ref - GWS::ERR:0204:MONID:GWS.NEXP.SVC MONSEV:B The threshold for third-party failures	INC6469861
Parent Incident			
INC6469861	19/10/2020 17:29:16	Internet Traffic Usage (GWS, CDP & HBS services)	

List of all incidents related to the issue raised by Fujitsu POA on 21.10.2020:

INC6485949	21/10/2020 12:06	GWS::ERR:0210:MONID:GWS.HLTY.ERROR MONSEV:B 22 requests failed in the last monit	INC6485885
INC6486044	21/10/2020 12:13	Branch Access and Collect and return showing critical on HORIce	INC6485885
INC6486129	21/10/2020 12:20	Internet Connectivity issues	INC6485885
INC6486171	21/10/2020 12:24	Critical 21-Oct-2020 11:54:45 BST NEOPOST- L4LB (IRE11) SERVICE IS DOWN No 21-Oct	INC6485885
INC6486268	21/10/2020 12:31	yslog.TCOMLoadBalancer TCOM_MONSERV:MONID:PGDD.SERVICE MONSEV:B DIAG 559	INC6485885
Parent Incident			
INC6485885	21.10.2020 12:00:41	Internet Traffic Usage (GWS, CDP & HBS services)	

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

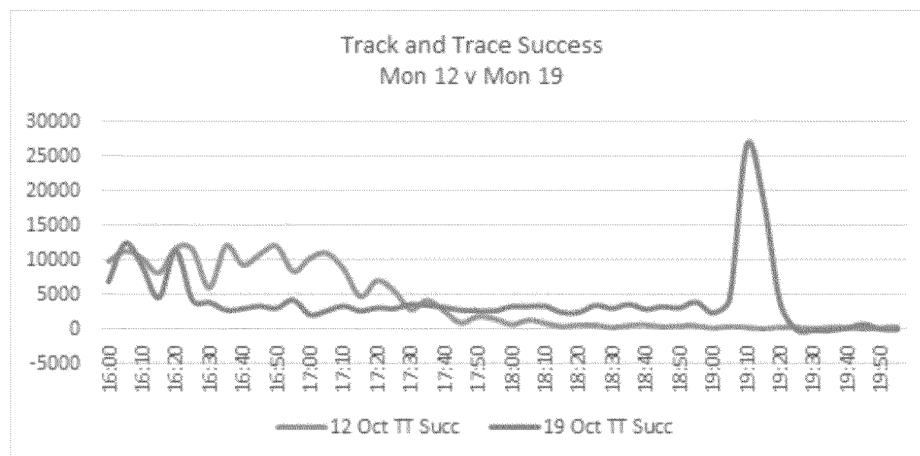
Peak Record: N/A

Change: N/A

IMPACT OF INCIDENT

Track and Trace (includes impact of simultaneous external incident in RMG domain):

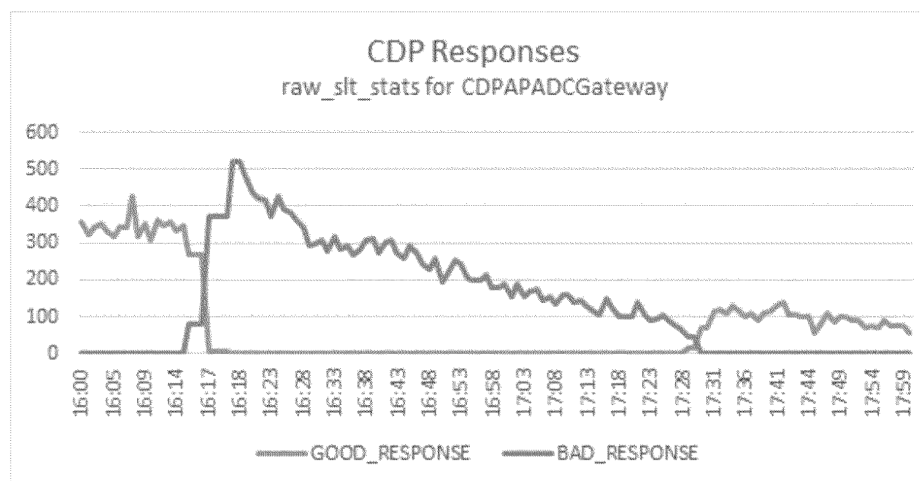
- SOAP faults 16:08 – 19:35
- T&T "success" stats comparison Mon 12 v Mon 19 16:00-20:00:



Overview
of Service
Impact
19.10.2020

CDP responses using the SLT_stats:

- Recovery at 17:30:



SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

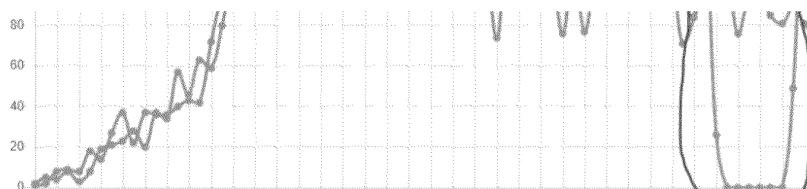
Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

RCode	Meaning	Counts
0	Success	10000
38	Error sending request (timeout)	182
80	Could not connect - unavailable	16512
82	Time out	122
98	CDP technical error	4
99	CDP business error	208
		27039

Service	Reqs received	Connctn fails	Timeouts	SOAP faults	Resps received	Success resps	Error resps	Resps returned
DVLA	1812	2	0	1	1809	1510	299	1812
FMCC / FMCV	1208	0	915	40	253	486	1	1208
HLTY	186	72	84	0	30	16	1	186
HPBB	26	0	11	0	15	6	9	26
NEXP	52	1	10	0	34	34	0	52
TOTAL	3284	75	1020	41	2141	2052	310	3284





SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

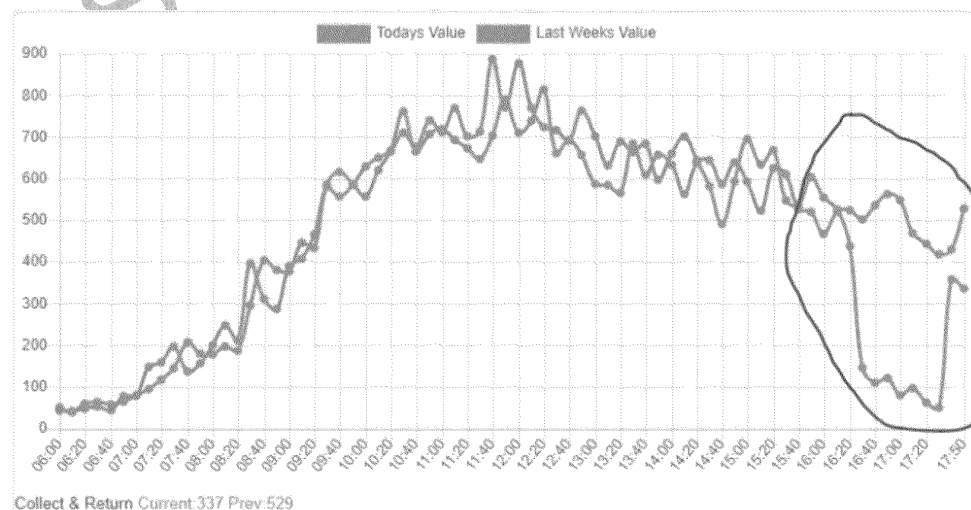
Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

Collect & Return comparison 19.10.2020



Overview of Service Impact 19.10.2020

PODG:

- Fujitsu observed alerts from multiple PODG routes between 17:15 and 17:39. Please see details in attached spreadsheet



PODG routes
affected.xlsx

BKAC

- BKAC time outs: 72
- First Response Code 82: 16:17
- First request post outage: 17:30
- No requests failed as service unavailable as h/c failing.

PCAI

- No impact – requests processed throughout

PGDD

- 3 Request time outs (Not a busy service)

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

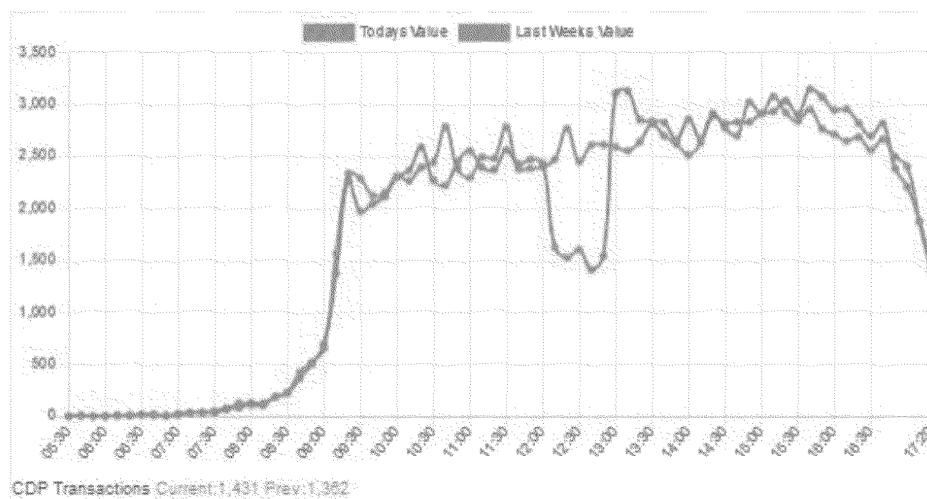
Peak Record: N/A

Change: N/A

**Overview
of Service
Impact
21.10.2020**

No impact to the counter estate directly, or Banking, EPOS, Card payments, or Track and Trace (impact to T&T on the 19th of October was a result of subsequent issue in RMG domain).

- CDP service degraded (comparison):



- Stat Counts for CDP between 11:00 – 13:00

RCODE	Meaning	Total
0	Success	20065
1		3
38	Error sending request, timeout	70
80	Could not connect	3080
82	timeout	40
84	invalid resp	1
98	CDP technical error	5

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

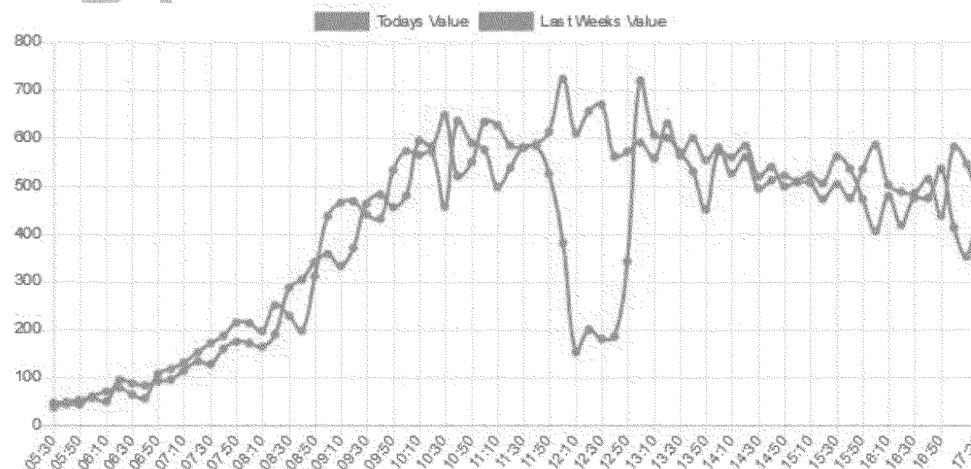
Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

**Overview
of Service
Impact
21.10.2020**

• **Collect & Return service degraded (comparison):**



Collect & Return Current: 485 Prev: 454

• **GWS services:**

- Summary counts between 11:50 – 12:55

SERVICE	Reqs received	Connctn fails	Timeouts	SOAP faults	% fail	Resps received	Success resps	Error resps
DVLA	1415	3	1	0	0.3%	1411	1222	189
FMCC	1210	0	1020	0	84.3%	190	378	1
FMCV	126	0	64	39	81.7%	23	23	0
HLTY	554	383	109	0	88.8%	62	38	2
HPBB	24	3	14	0	70.8%	6	0	6
NEXP	41	6	13	0	46.3%	20	20	2
TOTAL	3370	395	1221	39	49.1%	1712	1681	200

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

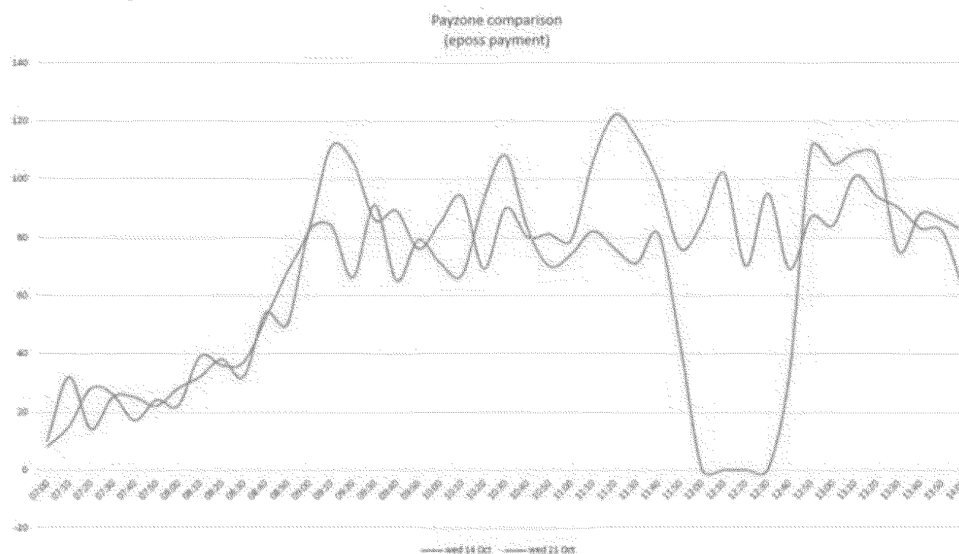
Peak Record: N/A

Change: N/A

**Overview
of Service
Impact
21.10.2020**

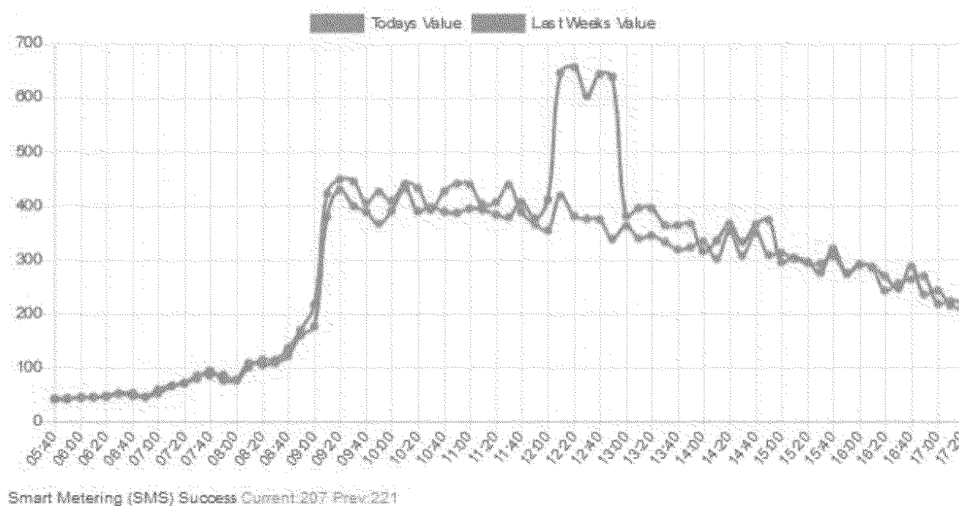
- **Payzone comparison with previous week**

- British Gas & Electric vends



- **Smart Metering (SMS)**

- This shows a spike in retries during the incident



SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

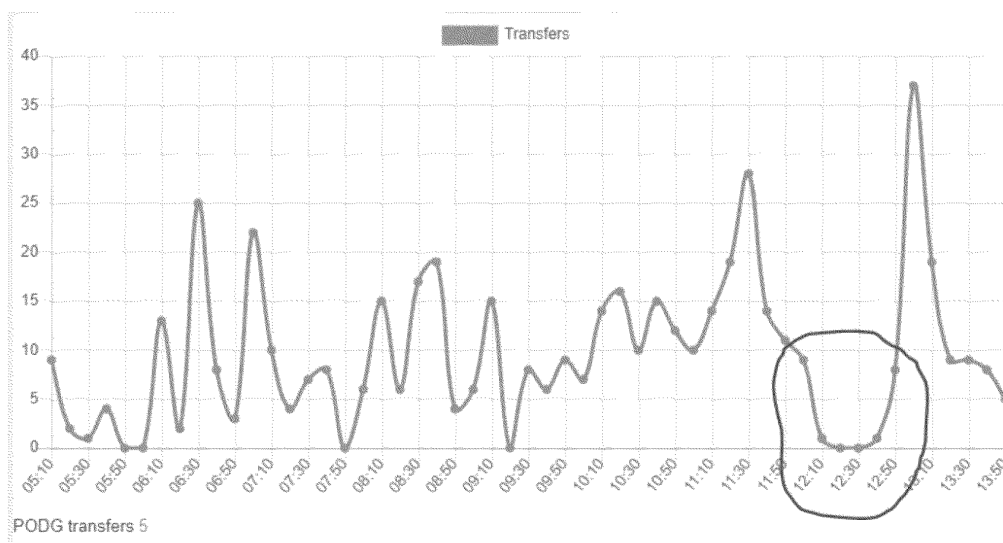
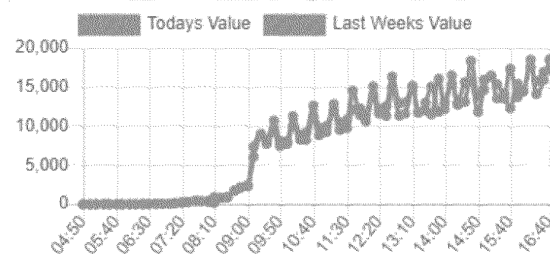
Problem Record: PRB0048676

Peak Record: N/A

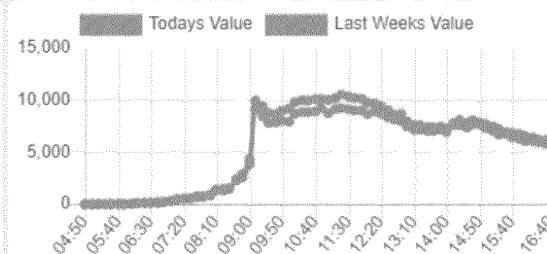
Change: N/A

**Overview
of Service
Impact
21.10.2020****• PODG transfers**

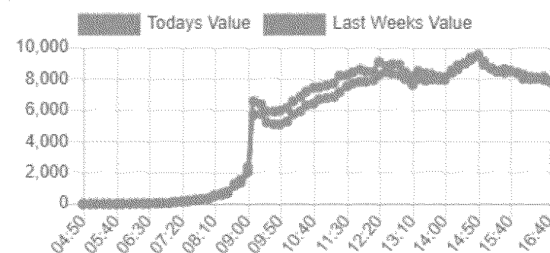
- All PODG file transfers completed successfully following restoration of the service (spike at 13:10 represents that)

**• Banking, Card Payments, APOP and Track & Trace remained unaffected:**

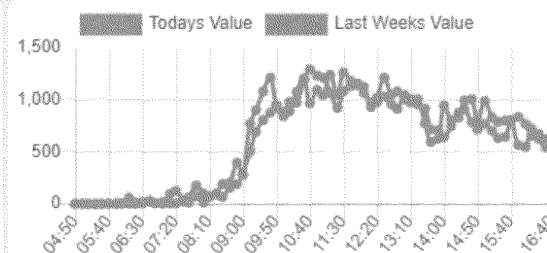
Track & Trace Current:18,591 Prev:17,199



Banking Transactions Current:5,552 Prev:6,085



Card Settlements Current:7,848 Prev:7,906



AP out payments Current:660 Prev:598

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

**Overview
of Service
Impact
21.10.2020**

- **BWS**
 - **BKAC – Bank Acct Checker**
 - **IRRELEVANT** BKAC.TIMEOUT MONSEV:B 18% (28 Timeouts in 154 requests)
 - **IRRELEVANT** BKAC.TIMEOUT MONSEV:B 11% (19 Timeouts in 162 requests)
 - No requests rec'd between: 11:55 and 12:45
 - **PGDD (guaranteed delivery)**
 - **IRRELEVANT** PGDD.TIMEOUT MONSEV:B 100% (1 Timeouts in 1 requests)
 - **IRRELEVANT** PGDD.TIMEOUT MONSEV:B 100% (1 Timeouts in 1 requests)
 - **PCAI – no impact**

**Overview
of
Business
Impact**

Please see statistics above.

COMMUNICATION METHOD

Email: Yes

Voice Calls: Yes

SMS: No

Bulletin: N/A

ACTIONS

No	Actions	Owner	Target Date	Comments / Updates	Peak
1	Fujitsu NOC Team continue to work with Juniper to understand the root cause and develop an action plan	Fujitsu NOC Shared Service s Team	23.10.2020	Completed 21.10.2020 – Further tests scheduled, investigation continues. 22.10.2020 – RCA for both incidents expected shortly.	N/A

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE



SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCE

Incident Date: 19 October 2020 and 21 October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

				<p>23.10.2020 – The following actions were completed on the 21st October to restore and resolve the root cause.</p> <ul style="list-style-type: none"> - Correct the commissioning error with the CenturyLink connection - Source replacement Hardware for failing component (router chassis) - Install replacement chassis and re-establish internet connections <p>Fujitsu technical SMEs to be physically on a Fujitsu Site for two weeks as a Hyper care measure.</p> <p>See Action 7 for further action plan.</p>	
2	Fujitsu POA to assess a full impact on Post Office Account services	Fujitsu POA	Completed 20.10.2020	<p>Completed</p> <p>Please refer to <i>Overview of Service Impact</i> section of this document.</p>	N/A
3	Fujitsu POA to conduct a Post Incident Review to identify improvements	Fujitsu POA	06.11.2020	<p>Completed</p> <p>21/10 – Awaiting outcomes of Fujitsu NOC investigation with the vendor (See Action 1)</p> <p>06/11 – A new process has been put in place for changes involving Fujitsu Critical Infrastructure. Senior Management and account teams will be informed and engaged, so that the Major Incident team have confirmed points of escalation during such changes.</p>	N/A
4	POA Problem Manager to raise a problem record to track the actions	POA Problem Manager	Completed 21.10.2020	<p>Completed</p> <p>Problem record PRB0048676 raised to track actions.</p>	N/A
5	POA UNIX removed the lockfiles on the PODG manually to allow the file transfers, rather than waiting for the automated process to run.	POA UNIX	Completed 19.10.2020	<p>Completed</p> <p>Completed during the POA bridge call.</p>	N/A
6	Fujitsu to confirm to POL regarding the POL traffics being observed on both routers	Sonia Hussain	Completed 30.10.2020	<p>Completed</p> <p>Sonia Hussain provided evidence to POL to demonstrate traffic on both prefixes.</p>	N/A
7	Fujitsu to confirm the disaster recovery plan	Fujitsu NOC Shared Services Team	Completed 12.11.2020	<p>Completed</p> <p>26/10 – Fujitsu are planning a change on the 10th and 12th November on the HSI routers where the resilience of the service will be tested. HSI Firmware Update CHG0201209 – LDC06, CHG0201213 – LDC08</p> <p>06/11 – The firmware upgrades on the Fujitsu High Speed Internet platform are</p>	N/A

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE

SECURITY CLASSIFICATION
COMMERCIAL IN CONFIDENCEIncident Date: 19 October 2020 and 21
October 2020

Version: 3.0

Owner: Piotr Nagajek

Status: Issued

POL Refs: INC0296097

Fujitsu Refs: INC6469861

Problem Record: PRB0048676

Peak Record: N/A

Change: N/A

				planned for the nights of Monday 9 th November (through to early hours on Tuesday 10 th November) and Wednesday 11 th November (through to early hours on Thursday 12 th November). 10/11 – CHG0201213 completed successfully with no impact to the service. 12/11 - CHG0201209 completed successfully with no impact to the service.	
8	POL shared an observation around speed of incidents being raised and escalated to POL MIM.	Sonia Hussain	Completed 27.10.2020	Completed For any Major Incident, POA DM will make a telephone call to POL MIM team immediately to notify them regardless of the incident ticket being raised.	

CLOSURE		
Date Closed	Fujitsu Approval	POL Approval
30.11.2020	Steve Bansal	Lorna Owens

For individual Major Incidents a Post Incident Review shall be held at which the Root Cause Analysis will be conducted and improvements considered from a lessons learnt perspective.

SECURITY CLASSIFICATION

COMMERCIAL IN CONFIDENCE