Data
Communications
Company

DCC Major Incident Review Report

Major Incident Description:	Central Switching Service Interruption of gate closure messages
Report Version:	2.0
Incident Date:	06/07/2023
Major Incident Ticket Reference:	INC0216074

Document Control

Documentation Control

Version	Date	Title	Author(s)
1.0	05/09/2023	DCC Major Incident Summary Report	Shona Wallace – Gibson
1.1	07/09/2023	DCC Major Incident Summary Report	Shona Wallace – Gibson
2.0	06/10/2023	DCC Major Incident Summary Report – Issued to RECCo	Luis Ogando

Documentation Reviewers

Name	Role
Lynette Jones	Head of Incident Management
Ian Drummond	Director of Customer Relationship Management

Report Distribution List

Company	Name	Job Title/Role	Method
REC	Performance Assurance Board		Electronic

Data
Communications
Company

DCC Major Incident Review Report – Central Switching Service

Date Of Incident	DCC Incident Reference Number	Service Impacted	Incident Reported Date/Time	Resolution Date/Time	Met with in SLA (Yes or No)	Time Taken to Resolve (In Hours)
06/07/2023	INC0216074	Central Switching Service – Interruption to Gate closure messages	06/07/2023 18:29	11/09/2023 16:06	No	1605.6 hours

Summary Report attached (Yes/ No)

Yes

DCC Resolver Teams and Service Providers involved

CSS Service Provider
Systems Integrator
SDSPs
DCC CTO
Working group of Core DCC personnel – Incident management, SMEs

Details of the impact of the Major Incident

The Business Continuity Disaster Recovery (BCDR) work that started in June, was scheduled to conclude on the 6 July 2023. The CSS Service Provider completed the failover from UK West (UKW) to UK South (UKS) following the runbook created for the failover process for BCDR.

At the 5pm Gate Closure (GC) on 6 July 2023, only 638 messages were sent out of CSS at GC rather than the expected ~60,000 messages.

Upon investigation, it was identified that the data expected in the queues, to process at this time, was incorrect. No data was lost, however the data that was needed to populate the queue with future dated gate closure messages was not readable and the switching data was unable to be loaded at the correct time. It was found that a replication issue with the queue meant switches with a supply start date of 7 July 2023 or later that had been submitted within the 28 days prior to 9am on the 6 July 2023 were unable to be processed.

Several options for fixing the impacted switches were assessed and the chosen solution was to requeue the messages that were due to be sent out. This solution was only adopted after technical reviews with industry and testing of the CSS Service Provider developed scripts.

Full impact has been confirmed as 200,756 switches and initial registrations. Parties did not initially receive GC messages for these switches and initial registrations. As a result, the end consumers did not have their switches fulfilled on the planned Supply Start Date.

Downstream billing for Gas Shippers was impacted for these switches due to the wrong supplier or shipper being attributed to the impacted meters.

39 incidents to the DCC Smart Metering Service centre were raised where gaining suppliers were unable to action 'Change Of Supplier' gains due to the Data Service Provider (DSP) system not recognising the gaining supplier as valid for the meters. This impacted prepayment customers with emergency meter installations carried out and a few cases experienced loss of supply for a short period of time.

Organisations had mobilised additional resource to support resolution activities including amending the impacted switches where suppliers submitted withdrawals after the Supply Start Date.

After rectification activities, two switches were in an incorrect state and needed to be withdrawn and resubmitted by the gaining suppliers. A final switch needed correction by the CSS Service Provider within CSS.

Detailed Action Taken

Date	Action	Description
06/07/2023	Incident occurred	- Gate closure completed in 53 seconds alerting Landmark of an issue. - Xoserve raised an incident indicating that Gate Closure messages for 6/7/2023 were missing. - Major Incident Management team mobilised. - Calls with DSP and Xoserve took place. - Initial view of impact (volume only) gathered and thought to impact 70k switches
06/07/2023	Incident communications commenced	Major Incident Communications including banner on portal was mobilised. This continued over the weekend including issuing comms to be shared on the REC Portal
11/07/2023	Initial customer calls held	Dedicated team established to liaise with industry parties (technical and governance)
12/07/2023	Daily portal communications frequency updated	- Daily portal communications continued, covering the following channels (3 times per day): - REC Portal - Service Now Portal
12/07/2023 (onwards)	Daily SOIF calls initiated	- Communications issued to all parties inviting them to attend daily SOIF calls. - Parties shared further insight with DCC expanding understanding of the full impact of the issue and allowed Landmark to carry out further detailed investigation into industry observations. - Technical solutions, timelines and processes developed and shared with industry for feedback and impact. - Parties explained technical issues associated with each option and solution agreed with industry collaboration. - All parties engaged that were impacted by the incident and allowing input into the decision-making process
13/07/2023	Initial impact presented	~193k switches and ~9k initial registration (for completeness the total number was subsequently confirmed to be 200,756 switches) - Exact number would not be knowing until after each Gate Closure as parties were able to withdraw future dated switches before each Gate Closure - Impact concentrated on 3 gaining suppliers who had ~84% of impacted switches. ~86% of switches had already past gate closure by the 13 July

14/07/2023	Joint briefing calls initiated	• Daily Bilateral calls between RECCo and DCC initiated
14/07/2023	Technical options presented	• Two proposed technical options were shared with industry for feedback: o Option 1: Cancellation (Withdrawal) of impacted switches (either centrally or by parties) o Option 2: Issue Gate Closure messages that had not previously been delivered. Subsequently: (Xoserve and MPRS confirmed impact of Option 1 without the need to carry out any testing) Xoserve confirmed that it could accommodate both options
17/07/2023	Testing approach presented	• UIT Test Approach proposed (for Gate Closure messages being issued – Option 2): o Number of participants requested. o Details of parties who would be simulated. o Data requirements o PKI requirements
18/07/2023	Data sharing approach shared	• Data shared via ServiceNow. • Data grouped by REC Party • Data elements and format explained
21/07/2023	Overall plan shared	• Plan showed 4 streams of activity: o Testing o Governance o Execution of Data Rectification o Post Fix activity (Data Reconciliation)
21/07/2023	Execution approach and principles shared	• Day 1: A small subset of switches to be processed through the technical option followed by validation activities that verified the actions taken have processed correctly before further switches initiated. • Further impacted switches to be processed in Chronological Order (earliest impacted SSD first) with no further prioritisation. • Batch sizes to be considered to ensure daily peaks were not exceeded
24/07/2023	UIT commenced	• Testing commenced with a single supplier with other suppliers being simulated by Netcompany as Systems Integrated

		• Some parties were unable to participate in testing due to not having sufficient environments and test certificates in place. • Some areas of testing were delayed due to there being no agreed approach to industry test management (environment readiness including test data set needing to be regularly updated and maintained and test certificates).
28/07/2023	UIT completed	• Test Completion Report (TCR) prepared outline the status of all planned tests. • TCR reviewed by DCC internal teams and Netcompany
31/07/2023	DCC option decision point agreed and presented to PAB and Industry.	• DCC determined that based on the testing results and a review by its architecture team, to plan for and implement technical option 2
02/08/2023	Execution of data rectification plan commenced	• Plan for data rectification showed activities showed detailed activities over the course of a 4-day execution window (illustrated below)
08/08/2023	Data rectification completed	• Data rectification completed on time as planned
11/08/2023	Data reconciliation approach shared	• Plan for detailed activities to be carried out as part of a reconciliation shared.

14/08/2023	Data reconciliation commenced	• Activities initiated in accordance with plan.
		• Streams of activity:
		  o Xoserve Reconciliation
		  o MPRS Reconciliation (Retrospective withdrawal errors)
		  o Failed to deliver.
		  o Customer raised incidents

21/08/2023	Industry 'Lessons Learned' commenced	• Online survey initiated using Third party application support forms
08/09/2023	Industry 'Lessons Learned' concluded	• 26 responses received
08/09/2023	Data reconciliation concluded	• No issues identified

Incident Escalated (Yes or No) If escalated, details of the Escalation

No

Information about any failures by Parties to comply with their obligations

N/A

Root Cause

The underlying cause has been attributed to an issue with load balancing due to a spike in Central Processing Unit (CPU) usage and Transactions Per Second (TPS) which contributed to a lag with Geo-replication across the regions. The load balancer was prioritising live traffic rather than the replication between regions.

When the Business Continuity Disaster Recovery (BCDR) came to failback the Storage and Application Accounts from the UK West (UKW) region back to the Primary UK South (UKS), replication had not completed to UKS before the failback was initiated. This caused current and future dated switches to remain unprocessed at Gate Closure.

Recommendations

It is recommended that the CSS Service Provider reviews the status of geo-replication daily, to ensure that no issues are present.

Additional alerts for geo synchronisation issues to be implemented so that any lag in last sync time is proactively investigated.

Updates to BCDR and Change runbooks to ensure that there are additional checks of queues throughout.

Review procedure to extract data from the system to ensure any data is available in a timely manner.

Action Plan to Address Root Cause / Preventive Actions

Item	Description	Owner	Closed	Open	Enterprise-wide Y/N
1.	Root Cause: Completion of RCA (Root Cause Analysis) investigations with CSS Service Provider and Third party application support	CSS Service Provider	✔		
2.	Mitigation: Confirmation of the chosen proposed solution option, two under review: • Option one is to cancel/withdrawal all impacted switches and for them to resubmitted either by parties or	CSS Service Provider/DCC	✔		

#	Description	Owner			
	through a central mechanism which has not yet been confirmed. • Option two is for CSS (Central Switching Service) to re-issue the secured active/inactive messages to all parties who should have received them.				
3.	Mitigation: • Completion of UIT (User Interface Testing) testing of the proposed solutions to correct the impacted switches/messages. • Market Participant / SDSP engagement to complete testing	CSS Service Provider/DCC/ Systems Integrator	✓		
4	Mitigation: • Completion of the identified solution to correct the impact for all switches / Switches in production	CSS Service Provider	✓		
5	Review of Comms tool for incidents	DCC		✓	
6	Architectural review: Future proof failovers, paper of options being put together by CSS Service Provider, e.g., backing up data to a third location	DCC/ CSS Service Provider		✓	
7	Mitigation plan should the issue reoccur	CSS Service Provider		✓	
8	Alerting on the geo replication synchronise last update time	CSS Service Provider	✓		
9	Confirm load balancing is not prioritising live traffic to the detriment of geo-replication.	CSS Service Provider/Third party application support		✓	
10	Has any of this CPU/Load Balancer behaviour been seen prior to 4th June?	CSS Service Provider/Third party application support		✓	
11	In future, CSS Service Provider will host a Third party application support engineer on their change bridge to provide assurance on the Azure environment. This practice was deployed on the Maintenance Release on the 16th of August with a successful outcome.	CSS Service Provider Third party application support	✓		
12.	Update monitoring and alerting around CPU use	CSS Service Provider	✓		
13.	Review the support model between CSS Service Provider and Third party application support	CSS Service Provider	✓		
14	Well architected Framework review between CSS Service Provider and Third party application support	CSS Service Provider		✓	

14.	REC/DCC review system requirements for SDSPs	DCC		✓	
15.	Understand if we can get sight of how many gate closure messages are expected for that specific day.	DCC		✓	
16.	Review of BCDR runbooks.	DCC		✓	
17.	Look at setting a threshold/ criterion for tickets to be raised off the back of last date/time sync monitoring.	DCC/CSS Provider		✓	

None

If there is likely to be a reduction in the DCC's External Costs arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time, please provide the details if available.

N/A

Potential REC Modifications

None

Details of the review of the response to the Major Incident and its effectiveness

Identification	The issue was identified as soon as Gate Closure completed due to the low volume of messages sent from CSS. A bridge call was setup with the relevant impacted parties to further quantify the impact.	🟩
Classification/Prioritisation	The incident was correctly prioritised as a Category 1 due to the impact this would have on market participants.	🟩
Investigation/Diagnosis	Initial investigations showed that there were gate closure messages not sent from the future dated queue. CSS continued to operate correctly for non-impacted switches and new registrations. The initial volume of impacted switches was estimated at ~202k, this volume was refined as the investigations progressed. Effectiveness AMBER as although the issue was understood in a timely manner, the full impact could not be quantified until after each respective Gate Closure.	🟧
Resolution/Closure	The selected solution was developed, tested and implemented in collaboration with industry. The execution completed as planned on 7 August 2023.	🟥

	Effectiveness RED due to the not meeting the SLA for the incident.	
Customer Communications	Customer communications have been sent out regularly with the impact and next steps clearly shown with updates on the actions.	