

---

# Office of Utilities Regulation

---

## FLOW OUTAGE REPORT

**PUBLIC VERSION**

2018 July 23



---

**OFFICE OF UTILITIES REGULATION**

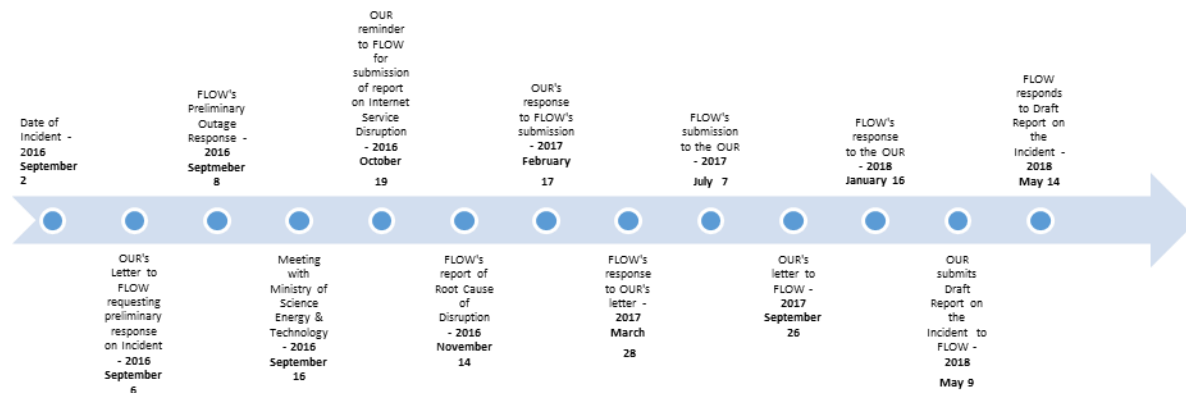
3<sup>rd</sup> Floor  
PCJ Resource Centre  
36 Trafalgar Road  
Kingston 10  
Jamaica  
West Indies

## Table of Contents

EXECUTIVE SUMMARY .....	2
1 INTRODUCTION.....	4
1.1 General.....	4
1.2 Purpose of Report.....	4
1.3 Background – Chronology of Events.....	4
2 DISCUSSION.....	6
2.1 OUR’s Analysis of Incident .....	6
2.2 Findings .....	11
3 CONCLUSION.....	12

## EXECUTIVE SUMMARY

This report details the OUR's examination and overall assessment of FLOW's submissions in relation to the outage which occurred on its network on the weekend of 2016 September 2 - 3 and which affected many of the company's customers. It outlines the sequence of events that transpired during that weekend based on the information submitted by FLOW in their report and feedback on the incident. The timeline below indicates the numerous exchanges between the OUR and FLOW in an attempt to get a clear understanding of the root cause of the event and to assure the OUR that the process and analysis undertaken by FLOW in the aftermath of the event provided the company itself with such an understanding.



*Figure 1 Timeline of Activities related to FLOW's Internet Disruption that occurred on 2016 September 2*

The series of exchanges between the OUR and FLOW was carried on over a timeframe of more than a year through both written and informal exchanges by way of telephone calls with FLOW on the matter. It notes that FLOW's account to the OUR on the incident was marked by protracted delays in providing several responses.

Additionally, the documentation provided to the OUR by FLOW does not, in the OUR's opinion, provide sufficient basis for corroboration of several of its findings.

All of this has served to weaken the level of confidence the OUR is able to place in the findings regarding the underlying root cause of the incident and the assurance against the occurrence of such incidences in the future. Consistent with the OUR's practice, FLOW has been given the opportunity to comment on a draft of this report and the OUR has considered those comments (including the company's reliance on the relevant statutory confidentiality provisions) in arriving at a final report for publication.

Arising from the actions and other inadequacies highlighted within this document, the OUR has concluded the following:

1. FLOW's conduct of the investigation and analysis and reporting on same have left critical questions unanswered and has materially compromised the OUR's ability to independently

assess, ultimately agree or otherwise with the findings presented as to the root cause of the outage.

2. The information provided on the remedial action taken by the company is insufficient to provide the requisite level of assurance to the OUR that the reoccurrence of this or a similar event is unlikely.
3. The OUR in issuing this report, is also indicating its concerns and dissatisfaction with FLOW's conduct of the investigation of its network failure and the possible implication for future outages. FLOW and other stakeholders should be guided by its content.
4. It is expected that FLOW will also give consideration to the issues raised in seeking to improve the resilience of its network and in undertaking any future root cause analysis into incidences on its network.

The OUR will also be furnishing a confidential version of the report to the Ministry of Science and Technology for its consideration and determination of any relevant action. As is the practice in such instances, a copy of the non-confidential version of the report will also be posted to the OUR's web site.

# 1 INTRODUCTION

## 1.1 General

The growth of the Internet and related services over the last few decades have been facilitated by the ability of consumers to obtain access through various devices including tablets, mobile phones as well as through various Customer Premises Equipment (CPE). Consumers typically rely on telecommunications operators to provide Internet access via their respective networks. The Internet is a vital medium of communication on which people rely for work, education, societal information and other critical activities. In that regard, the overall health of the networks that facilitate Internet access cannot be viewed as being simply the prerogative of the telecommunication operators themselves but rather as a matter of national concern. It therefore stands to reason that it is an imperative duty of the Office of Utilities Regulation (OUR) to thoroughly investigate any wide-scale interruption of access to Internet services, and a requirement of the relevant telecommunication operators to appropriately account for any such interruption of the services.

## 1.2 Purpose of Report

This report details the OUR's assessment of FLOW's report, including the root cause analysis which they have conducted, in relation to the events that transpired on the weekend of 2016 September 2-3 that led to the loss of Internet service to FLOW's customers. Arising from this, the OUR will indicate its own analysis of the information exchanged between the OUR and FLOW and state its conclusions regarding the same in keeping with its responsibilities under the Telecommunications Act (hereafter referred to as "the Act").

## 1.3 Background – Chronology of Events

On 2016 September 6, the OUR wrote to FLOW regarding reports of "extensive and wide-spread disruption of FLOW's Internet service" during the weekend of Friday 2016 September 02 to Saturday September 03. In this correspondence, the OUR noted that it had not received official notice of this significant event and stated that in keeping with its statutory mandate under sections 3 and 4(3) of the Act it would require that FLOW provide information on this incident. Specifically, the OUR required that FLOW provide a preliminary response by 2016 September 7, confirming whether the incident had occurred as well as providing other information related to the incident including:

- i. The time, extent and duration of the service outage;
- ii. Corrective/remedial action taken to address the outage, and restoration time;
- iii. Number of affected customers;

iv. Communication to customers regarding the outage (time, method).

In a letter dated 2016 September 8, and in response to the foregoing OUR request, FLOW confirmed the reported interruption of the company's Internet service and provided a brief account of the incident, including steps taken in determining the immediate cause of the problem and those taken to resolve it and restore service. Specifically, FLOW stated that on 2016 September 2 at 9:00 pm its staff received reports of a loss of connectivity at their facility which led it to conclude that there was an issue at its Network Operating Centre (NOC)/Data Centre in Kingston.

The letter further stated that subsequent investigation found that problems in the power systems had caused disruption to the data-provisioning platform, which resulted in an interruption of Internet Service to customers. The service interruption reportedly affected approximately 40,000 modems and 70,000 customers across several parishes including St. Catherine, Kingston & St. Andrew, St. James and Manchester. The company said that information on the service outage was communicated to its customers through its contact centre and a range of media outlets. FLOW also reported that the affected systems and service to its cable modem internet customers had been restored and that it would continue to monitor the network to ensure stability as well as continue its investigation of the matter. In a 2016 September 8 meeting, FLOW further advised the OUR that some aspects of its examination into the cause of the incident and the implementation of measures to mitigate the risk of future outages, were still ongoing.

On 2016 September 16, at a meeting convened by the Ministry of Science, Energy & Technology (MSET) and attended by FLOW and the OUR, to address the service interruption, the Minister called for a thorough and comprehensive investigation of the incident by FLOW. It was the view of the OUR that implicit in the Minister's call was the need for FLOW to adopt an investigative approach that would identify both the immediate and the underlying technical, procedural, administrative and/or human cause(s) of the incident. Thus, both the Ministry and the OUR emphasized that it was imperative that FLOW conducted an appropriate root cause analysis to support its investigation and reporting. Also at that meeting, the OUR requested to have sight of the expected incident investigation report to the Minister. FLOW in turn informed the meeting that it had commenced a root cause analysis (RCA) into the September 2 outage and subsequent smaller scale interruptions to its systems and gave an undertaking that it would share the results.

On 2016 October 19, the OUR gave FLOW a written reminder of the outstanding report and set 2016 October 31 as the deadline for its submission. On 2016 November 14, FLOW submitted a two and a half page letter with a limited account of the incident. The OUR issued a written response, which was copied to MSET, on 2017 February 17, indicating that FLOW's letter, which it was obliged to regard as its formal incident report, was largely inadequate in both form and substance. The OUR outlined its reasons for that assessment, noting that, among other things, given the extent of the service interruption, the regulator

of necessity should have been provided with a full, clear and unambiguous explanation of the event, identification of the underlying causes and the effectual measures, taken and to be taken, to prevent a recurrence and to protect the public interest.

The OUR further observed that whilst it acknowledged FLOW's reported efforts to arrest the problem and implement an immediate solution to restore service to affected customers, it was not satisfied that there had been an efficient and effective approach to the investigation of the incident in order to safeguard against a recurrence because of unresolved or inadequately addressed causal issues. The OUR also formulated and presented to FLOW a set of questions, which related directly to extracts from FLOW's previous correspondence, in order to obtain further clarity about what actually occurred and the immediate and root causes. However in its response, FLOW merely supplied its answers as in-line insertions against the questions instead of providing a substantive response to the issues raised.

FLOW subsequently acknowledged the shortcomings of its submission and agreed to refer the matter back to its technical support for further consideration and submission of the requisite incident report. A new report was submitted on 2017 July 07 but was deemed by the OUR to be also insufficient and not in the form required for the purpose. Consequently, the OUR wrote to FLOW on the 2017 September 26 detailing all the issues thus far identified and the attendant obligations placed on the service provider, and cautioned against non-compliance.

FLOW issued a response on 2018 January 16, in which it stated its disagreement with the Office's assertion regarding its submission on the outage incident. The company further stated that it has complied with the Office's request for the provision of a detailed accounting of the incident *"by way of letter, responses to the OUR's interrogatories and the submission of its internal Root Cause Analysis report"*.

As part of its 2018 January response, FLOW provided a copy of its *"Root Cause Analysis Report on the Disruption of Internet Service on September 2 & 3, 2016"* which was addressed to the Minister. The RCA report contains information related to the incident such as the remedial action taken by the company and FLOW's findings as to what it considered the root cause of the outage. The root cause was reported as being human error which was specifically attributable to a Tier 1 engineer on duty at the time.

## 2 DISCUSSION

### 2.1 OUR's Analysis of Incident

FLOW's response to this matter is lacking bearing in mind the following:

- i. the series of incidents that led to the request for a detailed report on the matter;
- ii. the number of subscribers impacted by the outage;

- iii. the interest in the matter taken by the Minister and other stakeholders; and
- iv. the overall importance of access to Internet services.

Furthermore, even with the robust engagement by the OUR, FLOW has failed to convince the OUR that it has engaged the level of investigative rigour that is required in matters of this nature. This assessment is based on the following:

- i. the information received by the OUR was found to be lacking in both form and content despite several requests for clarification from the OUR;
- ii. the gaps found in the sequence of events communicated by FLOW;
- iii. the conclusions reached by FLOW which were in some instances devoid of any corroborating evidence to support such conclusions; and
- iv. the overall treatment of a matter of such national importance.

These points are addressed in more detail in the analysis that follows which is consistent with the root cause analysis (RCA) methodology suggested by the OUR in reporting on the incident.

### **The Power System**

FLOW's submission on the incident suggests that the loss of commercial power to one of its locations triggered a series of events that resulted in the loss of Internet connectivity to a wide cross-section of FLOW's residential subscriber base. This loss of commercial power resulted in the supply of AC power being shifted to FLOW's redundant power system. Data centres typically require high levels of reliability and arrangements must be in place to support the services being provided by facilities housed at these locations. The question left unaddressed by FLOW in its analysis submitted to the OUR is the specific arrangements that were in place for ensuring that redundant power systems operate in the manner desired whenever normal commercial power arrangements are disrupted.

In its 2017 September 26 letter to FLOW, the OUR questioned the efficacy of the arrangements for power redundancy and stated that greater clarity was needed. The OUR also requested that FLOW provide clarity on several inconsistencies found in the RCA that it had submitted as a part of its incident report. FLOW's performance of a RCA was expected to identify the "root causes" of the outage as well as assist the service provider in mitigating the risk of similar outages in the future.

The OUR considers that this analysis would have been important in discovering what had transpired with several systems including FLOW's redundant power systems and further whether they failed and if so, why. These questions arose after looking at the configuration presented by FLOW in its line-diagram. The diagram showed several layers of redundancy present, including the presence of alternate power sources



as well as automatic transfer switches, within the power system that was in place at the Data Centre which leads to the questions of whether these systems had operated in the manner that had been specified by FLOW during the outage.

Moreover, the OUR considered it essential to know what had transpired to affect the orderly transfer of the load between the alternate power systems employed by the company. Indeed, based on the configuration displayed on the line-diagram submitted by FLOW and the subsequent instability reported by FLOW on one of its alternate power systems, more details would have been required for a meaningful assessment.

FLOW's response was not helpful as its statement that its technical team had attempted to transfer manually several devices, including parts of the data provisioning system, between the alternate power systems during the time of the outage only raised further questions. Essentially, it raised doubts about the effectiveness of the power switching systems used by FLOW and their role in achieving the level of redundancy required for such important facilities such as those found within FLOW's Data Centre. The OUR is therefore led to the conclusion that some issues exist with the overall redundancy configuration within FLOW's back-up power systems and the management of the redundant elements found within this redundancy arrangement. This could include issues related to the configuration of the adjustment delay mechanism that determines the length of time prescribed before reversion to the primary power source; the time taken to perform switching between the alternate power systems in order for a seamless transfer to be effected; among other factors. The information provided by FLOW is not, however, sufficient to allow for a more definitive pronouncement. The OUR urges FLOW to give further scrutiny to these matters, in its efforts to reduce the vulnerability and improve the resilience of its network and also in the conduct of any future root cause analysis.

Additionally, in the initial submissions made to the OUR, FLOW provided no indication of the nature of the initial alarm on FLOW's system to which the technician had responded. Information on the alarm condition was only revealed when the OUR specifically inquired about it. FLOW subsequently revealed the condition, which was observed at the time of the incident. However, no supporting data was given to clarify under what conditions such an alarm would arise and the likely effects the condition would have on the affected equipment, particularly where the condition causing the alarm is prolonged. It was therefore a matter of some concern that FLOW was not forthcoming in providing information on the matter. This raised doubts as to the level of effort employed by FLOW in bringing closure to the issue and the company's commitment to bringing to light the contributory factors that resulted in the outage. In so doing, deeper insights into the reasons for the outage could have been determined and the risk of occurrences of this nature reduced. Consequently the OUR is constrained to observe that the risk of recurrence remains in circumstances where conclusions reached by FLOW appear to have been predicated on a less than complete analysis.

Notably, in the OUR's email to FLOW on 2017 February 09, the question of the maintenance procedures utilised for the power equipment involved in the incident was raised, and in particular the failure of elements of FLOW's power system during the outage. The issue of maintenance ranks as a critical area of concern when seeking to manage "high availability" environments such as the Data Centre in which FLOW housed the affected power system and the parts of its broadband network affected by the outage. In its response, FLOW simply stated that it had performed planned power interruptions on these power systems as a part of earlier maintenance exercises with no subsequent failures being observed on the parts of the broadband provisioning systems that were impacted by the outage. However, this provides no sense of the rigour of the maintenance practices, especially when treating with complex power devices such as those found within FLOW's power system. This observation is based on the fact that such systems typically require varying degrees of analysis of several components, as well as functional load testing operating under steady-state and transient conditions,<sup>1</sup> in order to confirm proper operation of the device. Consequently, the response was not helpful to the OUR in identifying and isolating critical factors that may have caused the service disruption.

### **Broadband Provisioning Power Systems**

On the matter of the failure of the power system of the broadband provisioning system, it is noteworthy that the broadband provisioning system was attached to both the primary and secondary alternate power system deployed by FLOW. However, the broadband provisioning system did not seem to benefit from the redundancy provided by this arrangement. This again raises the question of the efficacy of the power arrangements and how their failure contributed to the damage to the platform. While there may be other factors that may have had a contributory effect on the outcome (which the OUR is not able to definitively address from FLOW's submissions), the question of the operation of the equipment must also be considered bearing in mind that it had been set up with several layers of redundancy which seemingly failed.

### **Human Intervention**

FLOW asserted in one of its submissions that the initial responder from the company, a technician, acted unilaterally and without authority in addressing an audible alarm that was indicative of a system fault. In the examination of the issue, it was also stated that the matter was an operational breach and that the technician seemingly acted improperly in discharging his duty in the matter. Absent information on the scope of the technician's authority and the specific responsibilities assigned to him; particularly where in this instance, he was the only person on site, the OUR is unable to opine further on this. Moreover,

---

<sup>1</sup> Curtis, P. (2007). *Maintaining Mission Critical Systems in a 24/7 Environment*. New Jersey, NJ: Wiley

although FLOW has termed the issue an operational breach, it has not referenced the issue to any specific procedural resource, such as an operational policy manual.

Furthermore, FLOW has made reference to internal investigations conducted in relation to the specific actions of the technician but has not provided the specific information and analysis which led to its substantive conclusion regarding the human error as the root cause of the failure seen in the power system. Again, absent such information the OUR is unable to express an independent opinion on the validity of FLOW's conclusion and the robustness of the process by which it has been arrived at.

### Chronology of events

Further to the points raised regarding the actions taken by the technician, there are also questions surrounding the precise timing of the events leading to the subsequent failure of the systems hosting the DHCP servers. This issue was highlighted in the OUR's letter to FLOW on 2017 September 26 that questioned the statement made in the Incident/Problem Review Template which read:

*"On September 2, 2016 at 18:00hrs, RNOC Tier 1 Jamaica received a report via the phone that person (sic) were experiencing loss of connectivity to the corporate network"*

However, in the same Incident/Problem Review Template, the Start and Stop times of Severity Levels, Outage and Incident Durations, the start time of *Severity 3* was listed as the same but the response time listed by the technician at the NOC was stated to be approximately 8:30pm. FLOW, in its submission, failed to reconcile the time reported and the subsequent response time listed by the technician, as well as the intervening events that had transpired during this period of time. The OUR is of the view that the series of events that transpired during the incident is material to establishing the causative factors contributing to the overall outage and urges FLOW to undertake that reconciliation.

Further, the timeline of activities included in the Incident/Problem Review Template, began with an entry for *2016 September 3 7:34hrs* reflecting the email notification that was sent by the RNOC Tier1 communicating that a problem was being experienced by broadband customers. There was no mention in the Incident/Problem Review Template of the activities preceding the email notification. The absence of this information is especially relevant when considering that the events concerning the power outage began from the day before. The OUR is of the view that the completeness of the timeline would have been critical to gaining a sense of the events that transpired up until the morning of the 2016 September 3 for the sake of determining other causative factors that may have contributed to the degradation of service and subsequent loss of service for subscribers. The OUR urges FLOW to close this informational or analytical gap in the efficacy of its findings.

## Follow up Action

The final submission by FLOW on 2018 January 16 stated that several activities were performed as a result of the outage that transpired on that weekend. In FLOW's submission, a list of several recommended actions taken by FLOW as well as the persons to whom these action items were assigned respectively, was shown. Along with the list of recommended actions, FLOW provided related narrative, stating what the company has termed to be "concise mitigation activities". This method of reporting however, has failed to provide much in the way of scale or scope of the remedial work undertaken by FLOW in addressing whatever shortcomings were identified during the course of their investigation.

Notably, FLOW has stated that it has introduced other redundancy mechanism into its network. However, limited information has been provided about the exact nature of this arrangement and how critical components of the network will be impacted under the new configuration bearing in mind the recent failure.

The issue of the introduction of additional redundancy is especially relevant bearing in mind that there were other systems that were also configured for redundancy that had seemingly failed to perform in the manner anticipated thereby leading to the loss of Internet service to many of FLOW's customers. This concern is relevant considering the operation of FLOW's alternate power systems, which included several automatic transfer switches, that were configured to provide greater system resilience and reliability but whose performance during the period of the outage was apparently questionable.

Additionally, as it concerns the primary alternate power system used by FLOW and its return to service, FLOW has not provided any information as to whether there will be any amendment to the existing maintenance procedures for elements of FLOW's power network arising from any shortcomings identified during the outage. The communication of such detail, would have allowed for greater transparency regarding the extent of the corrective actions taken on the system; and provided reassurance regarding the possibility of reoccurrences of this nature, and the chance of identifying and correcting any future deviations in the expected operations of these power systems in a timely manner.

## 2.2 Findings

Based on the analyses arising from the review of submissions by FLOW and related correspondence in relation to the activities surrounding the loss of Internet service to its residential customers on 2016 September 2-3, the OUR makes the following findings:

- There were material deficiencies in both the form and content of submissions by FLOW to the OUR with respect to the circumstances related to the outage which occurred on the weekend of 2016 September 2-3.

- FLOW's submissions of its RCA report omitted the vendor report on the equipment that was impacted during the incident, as well as FLOW's own internal report from Property Services. The provision of these reports would have placed the OUR in a better position to provide an assessment of the primary conclusions offered by FLOW regarding the extent to which human error contributed to the loss of power on FLOW's alternate power system and the subsequent damage suffered to the broadband provisioning system.
- There were critical inconsistencies in both the timeframe and the exact sequence of events surrounding the loss of Internet service on the weekend mentioned leading the OUR to question some of the conclusions reached by FLOW in relation to the outage as well as their assessment of its root cause(s). FLOW is urged to revisit these inconsistencies in the efficacy of its report.
- There is a clear need for a thorough review of the operation, maintenance and configuration of the primary and secondary elements of FLOW's backup power systems at the Data Centre in order to ensure optimal performance under varied operating conditions including those involving the loss of commercial power.
- A better understanding of the incident might have been gleaned if information was provided on the analysis of the power configuration for the impacted equipment and other elements of the overall broadband provisioning system impacted during the incident.
- The description of the corrective actions taken by the company does not allow for a proper assessment of their likely effectiveness in mitigating the possibility of future threats of this nature, as they have not clearly communicated how the stated improvements are intended to address shortcomings identified during the outage.

### 3 CONCLUSION

This incident has left a number of questions unanswered and there remains serious doubt as to whether the actions taken by FLOW will prevent a repeat of similar occurrences in the future. The OUR is aware that there have been several organizational and operational changes within the company and is concerned that these changes may have impacted FLOW's ability to adequately address the demands of its quality of service obligation. These changes carry attendant concerns related to the loss of organizational capacity and the increased likelihood of less than timely execution of critical procedures relating to the ongoing and regular maintenance of different network components, which are typically

highlighted during times of crisis. Based on the review of several submissions by FLOW and the exchanges between themselves and the OUR, the OUR has arrived at the following positions:

1. FLOW's conduct of the investigation, its reported analysis and the subsequent reporting of same, as well as the omission of several key documents, have left critical questions unanswered and has materially compromised the OUR's ability to assess and ultimately agree or otherwise with the findings presented as to the root cause of the outage. The OUR regards this as unsatisfactory, but believes the overall public interest will not be served by further delaying the release of this report.
2. The limited information provided on the remedial action taken by the company is insufficient to provide the requisite level of assurance to the OUR that the reoccurrence of this or similar event is unlikely.
3. In issuing this report, the OUR is indicating its concerns and dissatisfaction with FLOW's conduct of the investigation of its network failure and the possible implication for future outages.
4. The OUR expects that FLOW will be guided by the content of this report especially in respect of the information and/or analytical gaps in its submissions, the deficiencies indicated with respect to the conduct of its RCA and the reservation expressed with regard to the company's ability to mitigate and/or manage the risk of future such occurrences.

The OUR will also be furnishing a confidential version of the report to the Ministry of Science and Technology for its consideration and determination of any relevant action. As is the practice in such instances, a public version of the report will also be posted to the OUR's web site.