TAX APPEALS TRIBUNAL
Justice in Taxation

THE REPUBLIC OF UGANDA

IN THE TAX APPEALS TRIBUNAL AT KAMPALA

APPLICATION NO. 134 OF 2023

MTN UGANDA LIMITED.....APPLICANT

VERSUS

UGANDA REVENUE AUTHORITY.....RESPONDENT

BEFORE: HON. STELLA NYAPENDI CHOMBO, HON. PROSCOVIA REBECCA NAMBI, MS. CHRISTINE KATWE

RULING

I. Introduction

1. This is an application challenging an objection decision by the Respondent, which maintained an additional assessment of UGX 33,911,117,000 for Local Excise Duty on Over-the-Top (OTT) services. The dispute centres on alleged under-declarations for the period April 2020 to June 2021

II. Background Facts

2. The Applicant is a Ugandan company licensed to provide telecommunications and related services. The Respondent is the national tax authority vested with the mandate to assess and collect taxes in Uganda.

3. In the financial year 2017/2018, the Excise Duty (Amendment) Act 2018 was enacted, introducing a tax on Over-the-Top (OTT) services. Under Item 13(b) of the Second Schedule of the Act, the tax was prescribed at UGX 200 per user per day of access.

4. Section 2 of the Excise Duty (Amendment) Act 2018 defined "Over-the-top services" as the transmission or receipt of voice or messages over the Internet Protocol network, including access to virtual private networks (VPNs).

5. Prior to the implementation of the tax on July 1, 2018, stakeholders, including the Uganda Communications Commission (UCC), the Respondent, and telecommunications operators (including the Applicant), held several meetings to discuss the modalities of implementation. It was agreed that access to OTT services would be blocked for customers who had not paid the tax and granted upon payment of the tax.

6. To facilitate this, the Applicant operated a Policy and Charging Rules Function (PCRF) system designed to block non-compliant customers. Additionally, the Applicant maintained an Online Virtual Account (OVA) system that recorded OTT tax payments in real time and was accessible to the Respondent for revenue assurance purposes.

7. Between 2018 and 2022, the Respondent conducted a comprehensive audit of the Applicant. During this audit, the Respondent utilised data from a Data Monitoring System (DMS) also referred to as the Telecom Information Management System (TIMS) operated by Global Voice Group (GVG) on behalf of the Government of Uganda.

8. The Respondent's audit findings indicated a significant discrepancy between the OTT accesses recorded by the DMS and those declared by the Applicant.

Specifically, the DMS identified 308,793,188 unique OTT accesses, whereas the Applicant had declared 139,237,602, resulting in an alleged under-declaration of 169,555,586 accesses.

9. Consequently, the Respondent issued an additional administrative assessment for Local Excise Duty (LED) totalling UGX 33,911,117,000 for the period of April 2020 to June 2021. The Applicant objected to this assessment on April 25, 2023, contending, among other things, that there was no under-declaration and that the Respondent's methodology was flawed. On July 27, 2023, the Respondent issued a decision disallowing the Applicant's objections and upholding the assessment. Hence, this application.

III. Issues for determination

10. The following issues were agreed upon by the Parties for determination;
    a) Whether the Applicant is liable to pay the tax assessed?
    b) What remedies are available to the Parties?

IV. Representation and evidence

11. The Applicant was represented by Mr. Cephas Birungyi, Mr. Enoch Barata, Ms. Belinda Nakiganda, Ms. Linda Mugisha and Mr. Richard Agaba all of M/S Birungyi Barata and Associates. The Respondent was represented by Mr. Tonny Kalungi, Ms Gloria Twinomugisha, Ms. Eseza Victoria Sendege and Mr. Simon Peter Orishaba, all from the Respondent's Legal Services and Board Affairs Department.

The Applicant's evidence

12. The Applicant presented three witnesses, namely Mr. Vincent Muwonge (AW1), the Applicant's Senior Manager-Tax, Mr. Michael Kizza (AW2), the Applicant's Senior Data Planning Engineer and Telecommunications Engineer, and Mr. Mackinon Kabarole (AW3), the Applicant's Senior Manager

- Consumer Segment, who during the assessment period served as Senior Manager, Data Analytics and Reporting.

13. Collectively, the Applicant's witnesses testified regarding the introduction and implementation of the OTT tax, the Applicant's internal systems for collection and enforcement of the tax, the technical operation of the Applicant's telecommunications network, the audit and objection review processes, and the Applicant's challenge to the methodology employed by the Respondent in raising the impugned assessment.

14. The Applicant's case, as advanced through the three witnesses and the documentary evidence relied upon, was that the Applicant properly implemented and administered the OTT tax regime in accordance with the Excise Duty Act and the implementation directives communicated through UCC and URA. The Applicant contended that the Respondent's assessment was founded on a fundamentally flawed methodology that relied on traffic data captured from an inappropriate point within the telecommunications network, applied arbitrary analytical thresholds, failed to distinguish successful accesses from unsuccessful attempts, and relied on undisclosed business rules and assumptions which the Applicant was unable to verify independently.

Evidence of AW1 – Vincent Muwonge (Senior Manager – Tax)

15. AW1 adopted his witness statement as his evidence-in-chief and relied on various documents contained in the Applicant's Trial Bundle, including stakeholder meeting minutes, correspondence exchanged between the Applicant, URA and UCC, audit communications, objection notices, objection decisions, reconciliation records, assessment notices, and documents relating to the implementation and administration of OTT tax.

16. AW1 testified that when the OTT tax was introduced in July 2018, telecommunications operators faced significant uncertainty regarding

implementation because neither the Excise Duty Act nor any subsidiary legislation prescribed the technical mechanisms through which the tax was to be enforced. According to him, the implementation framework was therefore developed through extensive consultations involving URA, UCC, MTN, Airtel and other stakeholders.

17. According to the witness, those engagements resulted in the identification of the services that would constitute taxable OTT services, as reflected in Exhibit A1. He further testified that the tax return templates were redesigned to accommodate the reporting and remittance of OTT tax collections and that Online Virtual Accounts (OVAs) were established to facilitate remittance and reconciliation of the tax collected from subscribers. He referred the Tribunal to Exhibit A2 in support of this evidence.

18. He testified that throughout the implementation period, telecommunications operators consistently raised concerns relating to VPN usage, postpaid customers, corporate subscribers, public internet access points, roaming customers, and the practical definition of OTT access. According to AW1, operators repeatedly informed regulators that VPNs were dynamic and constantly evolving and that it would be technically impossible to eliminate all VPN-enabled access to OTT services. He referred to correspondence and meeting records showing that these concerns were discussed extensively with both UCC and URA.

19. The witness testified that each telecommunications operator was permitted to utilise its existing technological infrastructure to collect the tax provided that the agreed implementation objectives were achieved. He referred to Exhibits A3 and A4 and explained that the Applicant implemented a mobile money-based payment solution through which subscribers elected to pay the tax before accessing OTT services. He further referred to Exhibit A6 and stated

that the Applicant's system was configured to ensure that OTT access could only be activated after payment had been successfully received and validated.

20. AW1 testified that during stakeholder engagements, it was further agreed that the phrase "per day of access" would be operationalised as a rolling twenty-four-hour period rather than a calendar day. He referred to the relevant stakeholder records and correspondence and stated that once a subscriber paid the OTT tax, access remained available for twenty-four hours from the time of payment.

21. AW1 further testified that the Applicant implemented systems designed to ensure that OTT tax was collected before subscribers could access OTT services. A subscriber required two conditions to be met before accessing OTT services through the Applicant's network. First, the subscriber had to possess a valid internet bundle or data package. Secondly, the subscriber had to have paid the applicable OTT tax. According to the witness, subscribers who had not paid the tax were automatically blocked from accessing OTT services through the Applicant's enforcement systems. He stated that every OTT payment was linked to a unique International Mobile Subscriber Identity (IMSI), thereby enabling the Applicant to trace each payment to a specific subscriber.

22. According to him, the Applicant consistently declared and remitted OTT tax collected from subscribers and maintained records of subscriptions and payments. AW1 testified that the Applicant collected and remitted all OTT tax paid by subscribers during the period the tax was in force. He produced evidence showing that the Applicant remitted UGX 12,688,588,400 in 2018, UGX 26,638,957,280 in 2019, UGX 28,319,181,820 in 2020, and UGX 6,659,669,534 in 2021.

23. AW1 challenged the Respondent's assertion that the Applicant had under-declared OTT accesses by more than 139 million accesses during the

assessment period, resulting in the additional assessment of UGX 33,911,117,000. He testified that the assessment was founded on assumptions that were neither supported by the law nor by the Applicant's network records. In particular, he stated that the Respondent adopted a data movement threshold of 1KB per day, having previously referred to a threshold of 1MB, as the basis for determining access to OTT services. According to the witness, no such threshold was prescribed under the Excise Duty Act, discussed during stakeholder engagements, or agreed upon as part of the implementation framework for the tax.

24. The witness further testified that the Respondent's data was obtained through a probe installed within the GPRS Tunnelling Protocol (GTP) region of the network. He maintained that this was technically inappropriate because the Applicant's access controls were enforced at the Gi region of the network, where internet traffic is ultimately processed and regulated. In his view, data obtained from the GTP region could not reliably establish whether a subscriber had actually accessed an OTT service, because that region also captures signalling traffic, unsuccessful attempts, and other forms of network activity that occur before access controls are applied.

25. AW1 further identified several inconsistencies within the Respondent's dataset. He testified that the Respondent recorded network activity for certain subscribers whose corresponding Call Detail Records reflected zero bytes of usage. He further stated that the total OTT payload reflected in the Respondent's analysis exceeded the total payload recorded across the Applicant's access network, a result he considered technically impossible. He also testified that the Respondent failed to account for the twenty-four-hour overlap adopted during implementation and therefore risked counting accesses in a manner inconsistent with the agreed operational framework.

26. AW1 testified that during the audit and objection review process, the Applicant repeatedly sought disclosure of the data, methodologies, business rules and assumptions used by the Respondent. He referred to correspondence in which the Applicant requested IMSI-level information, details of the subscribers allegedly accessing OTT services without payment, the underlying datasets relied upon by the Respondent, and the business rules used to transform captured traffic into taxable accesses.

27. According to AW1, the information disclosed by the Respondent was insufficient to permit meaningful verification of the assessment. He maintained that the Respondent provided only summaries and limited samples of processed data while withholding the complete datasets, algorithms, business rules and analytical assumptions necessary to reproduce the assessment.

28. During cross-examination, AW1 acknowledged that he was not a telecommunications engineer and that certain aspects of the Applicant's technical challenge depended upon the evidence of AW2 and other technical personnel. He further acknowledged that the Government's monitoring systems captured information from MTN's network and that the Applicant did not possess all of the datasets obtained through those systems. He also acknowledged that some concerns raised by telecommunications operators were addressed through engagements with the UCC and the URA, although he maintained that important concerns remained unresolved.

29. Notwithstanding those concessions, AW1 maintained that the central issue was not whether the monitoring systems collected information from MTN's network but whether the Respondent's methodology accurately distinguished successful OTT accesses from unsuccessful attempts and whether the resulting assessment could be independently verified.

Evidence of AW2 – Michael Kizza (Senior Data Planning Engineer)

30. AW2 was the Applicant's principal technical witness. He adopted his witness statement and relied on technical diagrams, network architecture illustrations, demonstration videos, VPN records, and documentation describing the operation of MTN's OTT enforcement infrastructure.

31. AW2 explained in considerable detail the architecture of MTN's network and the technical controls implemented to enforce the OTT tax. He testified that the Applicant deployed an integrated architecture comprising a Policy and Charging Rules Function (PCRF), a Policy Control and Enforcement Function (PCEF), mobile money systems, subscriber databases, and charging systems.

32. According to AW2, the PCRF and PCEF operated together as a central enforcement mechanism referred to during the proceedings as the "Gateman." According to the witness, the system's objective was to ensure that access to OTT services could be granted only after confirmation that the relevant tax had been paid. He testified that every subscriber was blocked from accessing OTT services by default and that access would be granted only after the PCRF verified payment of the OTT tax and communicated an authorisation decision to the PCEF.

33. AW2 emphasised that the Applicant's architecture was designed to prevent successful OTT access in the absence of payment. In his view, this was the most important technical feature of the implementation framework because it meant that any methodology seeking to determine whether OTT tax had been paid needed to account for the operation of the PCRF and PCEF systems.

34. A substantial portion of AW2's evidence concerned the distinction between the GTP region and the Gi region of the telecommunications network. Using technical diagrams and demonstrations, he explained that traffic captured in the GTP region includes signalling traffic, failed connection attempts,

retransmissions, background communications between applications and network elements, and traffic generated before the Applicant's access controls are applied.

35. By contrast, the Gi region lies downstream of the enforcement mechanisms and therefore contains traffic that has successfully passed through the Applicant's controls. AW2 testified that successful OTT access can only be confirmed after traffic has passed through the PCRF/PCEF enforcement point.

36. According to AW2, the Respondent's methodology was fundamentally flawed because it relied on information captured from the GTP region. He testified that traffic visible at that point may include users who attempted to access OTT services but were blocked due to non-payment, insufficient airtime, expired subscriptions, inadequate data bundles or other technical reasons.

37. AW2 also testified regarding VPN traffic. He explained that VPN applications continuously evolve and employ techniques designed to evade detection. Although the Applicant invested significant resources in identifying and blocking VPN traffic, complete elimination of VPN-enabled access was technically impossible. He testified that the Applicant regularly updated VPN signatures and maintained VPN protocol lists throughout the implementation period.

38. During cross-examination, AW2 acknowledged that he had not personally participated in the stakeholder consultations that led to the introduction of the OTT tax. He further accepted that the Government monitoring probes physically collected information from MTN's network and that the traffic relied upon by the Respondent originated from the Applicant's systems. He also accepted that the demonstration video tendered by the Applicant had been edited, although he maintained that the edits merely synchronised recordings and did not alter the substance of the demonstration.

39. AW2 further stated that VPN traffic could not be completely blocked and that some VPN-enabled accesses may have occurred despite the Applicant's enforcement efforts. Nevertheless, he maintained that the existence of VPN traffic did not justify treating all traffic observed in the GTP region as successful OTT access.

40. During re-examination, AW2 reiterated that his criticism was directed at the Respondent's methodology rather than the existence of the monitoring system itself. He maintained that the central technical question was whether the information captured before the enforcement controls could reliably establish successful OTT access.

Evidence of AW3 – Mackinon Kabarole (Senior Manager – Consumer Segment)

41. The Applicant further called Mr. Mackinon Kabarole (AW3), the Senior Manager – Consumer Segment at MTN Uganda Limited. AW3 adopted his witness statement, which was admitted as Exhibit AW3. He relied on correspondence exchanged between the Applicant and the Respondent, stakeholder meeting records, audit and objection review documents, reconciliation materials, OVA-related records, VPN-related communications, sample datasets disclosed by the Respondent, and other documents contained in the Trial Bundle.

42. AW3 testified that during the period under assessment, he was responsible for Data Analytics and Reporting and was therefore familiar with the Applicant's data management systems, reporting structures, and the implementation of the OTT tax regime. His evidence principally concerned the methodology employed by the Respondent in arriving at the impugned assessment and the Applicant's objections thereto.

43. The witness testified that following the introduction of the OTT tax, the Applicant implemented the requirements communicated through UCC and URA, including the deployment of a Policy and Charging Rules Function (PCRF) within its network. According to AW3, the PCRF functioned as a gatekeeping mechanism that permitted access to OTT services only after verification that the applicable OTT tax had been paid. It was his evidence that the system operated automatically and applied uniformly to all subscribers.

44. AW3 challenged the Respondent's reliance on information obtained through the monitoring systems implemented by Global Voice Group (GVG). He testified that the Respondent's analysis was based on information extracted from the Applicant's network's GTP region. According to the witness, the GTP region captures signalling traffic, retransmissions, failed connection attempts and other forms of network activity generated before access-control mechanisms are applied. In his view, the presence of traffic within that region does not necessarily establish successful access to OTT services.

45. The witness contrasted the GTP region with the Gi region, which he described as the point at which access controls are enforced, and actual internet access occurs following verification through the PCRF system. He maintained that any assessment intended to determine taxable OTT access ought to have relied upon information obtained from the Gi region rather than the GTP region.

46. In support of his evidence, AW3 referred to Figures 3 and 4 annexed to his witness statement. He testified that the figures illustrated differences between the Respondent's extracted sample data and the Applicant's network records. He further testified that the Respondent employed traffic thresholds as indicators of OTT access. According to the witness, the Respondent initially referred to a threshold of 1 megabyte (1 MB) and subsequently relied on a threshold of 1 kilobyte (1KB). It was his evidence that neither threshold was

prescribed by statute, subsidiary legislation, nor agreed upon during stakeholder engagements.

47. AW3 also questioned the statistical basis of the assessment. He testified that the Respondent extrapolated liability covering approximately fifteen months from a sample comprising only five days of network activity. According to the witness, the Applicant neither participated in nor agreed to the sampling methodology and was not provided with evidence demonstrating that the sample was representative of network activity throughout the assessment period.

48. The witness further testified that his review of the sample data disclosed by the Respondent revealed a number of anomalies. Referring to Figure 1 in his witness statement, he stated that several IMSIs appearing in the sample did not conform to MTN's standard fifteen-digit IMSI structure. He explained that IMSIs are unique subscriber identifiers and that irregularities in those identifiers raised concerns regarding the reliability of the underlying dataset.

49. AW3 further referred to a table appearing in his witness statement showing 158,840 IMSIs for which the Respondent recorded network activity while the Applicant's records reflected no corresponding usage. He testified that this discrepancy suggested inconsistencies between the Respondent's data and the Applicant's own records. He also referred to Figure 2, which analysed traffic volumes contained in the sample data and indicated that approximately 65 per cent of the identified IMSIs generated less than one megabyte of traffic over an entire day. According to the witness, such traffic volumes were inconsistent with normal OTT usage and suggested that signalling traffic, unsuccessful attempts or other non-OTT activity may have been included in the Respondent's analysis.

50. With regard to the identification of OTT services, AW3 referred to correspondence obtained from Meta Platforms Inc. and to Exhibit A16. He testified that certain IP addresses relied upon by the Respondent as belonging to OTT services did not appear to correspond with Meta-operated platforms and that some addresses relied upon in the assessment did not appear on official lists of OTT service addresses. In his view, these matters raised concerns regarding the accuracy of the Respondent's OTT identification methodology.

51. The witness also addressed the treatment of VPN traffic. Referring to Figure 5 and related correspondence, he testified that the Respondent's sample data appeared to include VPN-related traffic, notwithstanding stakeholder discussions regarding the treatment of VPN usage during implementation of the OTT regime. According to the witness, inclusion of such traffic would affect the reliability of the assessment.

52. AW3 further testified that throughout the audit and objection review process, the Applicant repeatedly requested disclosure of the datasets, business rules, analytical models and computations used by the Respondent in generating the assessment. According to him, the Respondent disclosed limited sample data but did not provide the complete methodology or underlying workings necessary to enable a full reconciliation of the assessment.

53. During cross-examination, AW3 acknowledged that the Applicant participated in stakeholder engagements concerning implementation of the OTT tax regime and that some concerns raised by telecommunications operators were addressed through engagements with UCC and URA. He also accepted that VPN usage could not be completely eliminated, notwithstanding the Applicant's efforts to identify and block VPN applications.

54. The witness further acknowledged that VPN reports relied upon by the Applicant were not tendered as exhibits before the Tribunal. He also acknowledged that he could not personally identify the precise subscriber base underlying certain revenue figures referred to during the proceedings.

55. AW3 further acknowledged that the Respondent requested GGSN data, IMSIs, IP addresses and payload information during the audit process. He maintained, however, that the Applicant supplied all information requested and that no communication was received indicating that the information supplied was incomplete. He also stated that the Respondent explained aspects of its methodology during reconciliation meetings, including the use of a 1KB threshold, although he maintained that the Applicant consistently disagreed with that methodology. The witness further accepted that GVG may have obtained information from the Applicant's systems, although he maintained that the information was not obtained directly from the Applicant.

56. In re-examination, AW3 reiterated that the Applicant's principal objection concerned the reliability of the methodology used by the Respondent to convert captured network traffic into taxable OTT accesses. He maintained that successful OTT access could only be confirmed after traffic had passed through the Applicant's enforcement mechanisms and that the Respondent had not demonstrated that identifiable subscribers accessed identifiable OTT services without payment of the prescribed tax.

57. The witness therefore maintained that the assessment was founded on assumptions, undisclosed methodologies, unverified thresholds, and data whose reliability remained disputed. He accordingly urged the Tribunal to set aside the assessment.

The Respondent's evidence

58. The Respondent's case was presented through two witnesses, namely Mr. Laurent Fiacre Sarr (RW1), a Telecommunications Engineer and Senior Consultant involved in the implementation and operation of the Government of Uganda's Telecom Information Management System (TIMS) and Data Management System (DMS), on behalf of Global Voice Group (GVG) and Mr. Grace Aine Ngabirano (RW2), the Manager Tax Risk at the Uganda Revenue Authority (URA) who participated in both the audit and objection review processes that culminated in the impugned assessment. Through these witnesses, the Respondent sought to establish the technical basis on which telecommunications data was collected and analysed, the methodology employed to identify OTT accesses, the audit process that culminated in the assessment, and the basis on which the Applicant's objections were rejected.

Evidence of RW1 – Laurent Fiacre Sarr (Telecommunications Engineer and Senior Consultant, Global Voice Group)

59. RW1 adopted his witness statement and relied on several technical documents, including the High-Level Design Document for the Data Monitoring Solution, DMS process-flow diagrams, network architecture schematics, demonstration videos, sample datasets, technical presentations and reports generated from the Data Monitoring System.

60. RW1 testified that he was involved in the deployment and operation of the Government's telecommunications monitoring infrastructure and was familiar with both the architecture and operation of the Telecom Information Management System (TIMS) and the Data Monitoring System (DMS).

61. According to RW1, the monitoring platform was introduced because Government agencies previously relied almost entirely on declarations submitted by telecommunications operators and lacked an independent means of verifying the accuracy of those declarations. He testified that the

TIMS and DMS platforms were designed to provide the Government with an independent source of telecommunications data capable of supporting revenue assurance, regulatory oversight and compliance verification.

62. The witness explained that the DMS captures information directly from telecommunications networks through probes installed at specific points within the operator's infrastructure. Referring to the High-Level Design Document and the architecture diagrams in the Trial Bundle, he testified that data is collected from the Gn/Gp and S5/S8 interfaces because those interfaces preserve subscriber-level information necessary to identify individual users and to associate traffic with particular subscribers.

63. RW1 explained that the Gi interface was not selected as a collection point because Network Address Translation (NAT) causes multiple subscribers to share a single public IP address, thereby making subscriber identification difficult. According to him, the Gn/Gp and S5/S8 interfaces retain identifiers such as IMSIs, MSISDNs, PDP Context information and IP assignments, enabling traffic to be correlated with individual subscribers.

64. The witness testified that the selection of these interfaces followed technical consultations involving UCC, URA and telecommunications operators and was informed by the objective of obtaining subscriber-level visibility. He maintained that the collection points adopted by the DMS were the most reliable locations within the network for compliance monitoring.

65. RW1 explained the operation of the DMS in considerable detail. He testified that the system captures both signalling traffic and payload traffic from the telecommunications network. The captured information is subsequently processed through several analytical stages. During pre-processing, subscriber identifiers are correlated with traffic sessions and payload records.

The system thereafter applies a series of analytical rules, filters and validation procedures intended to distinguish OTT traffic from ordinary internet traffic.

66. According to RW1, OTT identification is not based on a single indicator. Rather, the DMS employs a combination of factors, including destination IP addresses, application certificates, proprietary protocols, traffic flow characteristics, bandwidth consumption patterns, and other technical indicators. It was his evidence that the system continuously evolves to accommodate changes in the infrastructure of OTT service providers.

67. RW1 further testified that the DMS categorises traffic into several distinct classes, including Unique OTT Accesses, Unique VPN Accesses, Unique OTT and VPN Accesses, Non-OTT Traffic and Blocked OTT Attempts. He explained that VPN traffic is separately identified and segregated from OTT traffic, and that blocked attempts are not treated the same way as successful accesses.

68. A substantial portion of RW1's evidence was directed towards explaining the distinction between the DMS and the Applicant's PCRF/PCEF infrastructure. He testified that whereas the Applicant's systems are designed to control and enforce access restrictions, the DMS serves a fundamentally different purpose, namely the independent monitoring and analysis of telecommunications traffic. In his view, the Applicant's criticism of the DMS was based on an incorrect assumption that the monitoring platform should replicate the functions performed by the Applicant's internal enforcement systems.

69. The witness also testified regarding the provenance of subscriber identifiers. He explained that the DMS does not generate IMSIs or create subscriber information but merely captures information originating from the operator's network. Accordingly, any anomalies appearing within the captured datasets

would necessarily originate from the source network rather than from the DMS itself.

70. RW1 conducted demonstrations before the Tribunal using videos and live system displays. Through these demonstrations, he illustrated how probes collect signalling traffic and payload information, how subscriber identifiers are associated with network sessions, how information is stored within the DMS environment and how compliance reports are generated. He testified that the underlying data is stored within a Cassandra database and undergoes several stages of processing before becoming available for analysis and reporting.

71. The witness also referred extensively to the High-Level Design Document for the Data Monitoring Solution. He described the document as the principal architecture document governing implementation of the monitoring platform and testified that it remained operative at the time of the hearing. He further stated that the platform was owned by the Government of Uganda and maintained by the Uganda Police Force, and that access to the platform was available to institutions such as URA, UCC, and the Bank of Uganda for purposes consistent with their respective statutory mandates.

72. During cross-examination, RW1 acknowledged that the demonstrations shown to the Tribunal were based on data generated in July 2025 rather than data from the assessment period. He explained, however, that the demonstrations were intended to illustrate the operation of the DMS and not to reproduce the actual datasets used in the assessment.

73. RW1 further acknowledged that the Respondent does not retain raw signalling data after processing and stated that, as a technical matter, errors may potentially be introduced during data processing. He nevertheless maintained that the DMS employs established methodologies intended to preserve the integrity and reliability of the processed data.

74. The witness also stated that the DMS does not independently verify whether a subscriber paid OTT tax before identifying an OTT access. According to him, the role of the DMS is to identify network activity and access, while verification of declarations and tax payment forms part of a separate compliance process.

75. RW1 further acknowledged that traffic captured within the GTP region includes both successful and unsuccessful attempts. He maintained, however, that the DMS applies additional filtering and validation procedures intended to distinguish successful accesses from unsuccessful attempts and other forms of traffic.

Evidence of RW2 – Grace Aine Ngabirano

76. RW2 adopted his witness statement and relied on audit reports, assessment notices, objection decisions, reconciliation records, correspondence exchanged between the parties, sample datasets, internal analyses and other documents generated during the audit and objection review processes.

77. RW2 testified that he participated in the audit, which culminated in the impugned assessment, and was also involved in the subsequent objection review process. His evidence principally concerned the manner in which the information obtained through TIMS and DMS was utilised during the audit and the basis upon which the Applicant's objections were rejected.

78. According to RW2, analysis of data obtained through the monitoring systems revealed a significant variance between OTT accesses identified through DMS and accesses declared by the Applicant for Local Excise Duty purposes. He testified that the Respondent compared the independently generated DMS reports with the Applicant's declarations and concluded that a substantial number of OTT accesses had not been declared.

79. RW2 explained that the assessment was not based solely on raw traffic captured by the monitoring platform. Rather, the Respondent relied upon processed reports generated after application of the DMS methodology. He testified that the Applicant was afforded an opportunity to review sample datasets and participate in reconciliation exercises during both the audit and objection review stages.

80. The witness testified that the Respondent adopted a rolling twenty-four-hour methodology whereby a subscriber was counted once within a twenty-four-hour period commencing from the first identified OTT access. According to him, the methodology was intended to prevent duplication and ensure consistency in the counting of accesses.

81. RW2 also explained the basis for the one-kilobyte threshold relied upon by the Respondent. He testified that the threshold was developed through analysis of network activity and was intended to distinguish successful OTT sessions from signalling traffic and blocked attempts. According to him, unsuccessful attempts generally generated traffic volumes below that threshold.

82. The witness further testified that the Respondent did not rely exclusively on IP addresses in identifying OTT traffic. He stated that the methodology incorporated several indicators, including application certificates, proprietary protocols, traffic signatures and traffic-flow characteristics.

83. RW2 testified that the Respondent considered each of the objections raised by the Applicant, including concerns relating to VPN traffic, IMSI anomalies, unsuccessful attempts, disclosure of methodology and traffic thresholds. According to him, those concerns were analysed during the objection review process and were found not to invalidate the assessment.

84. During cross-examination, RW2 acknowledged that the one-kilobyte threshold was neither prescribed by statute nor by formal stakeholder agreement and that it formed part of the Respondent's analytical methodology. He also acknowledged that the Respondent extrapolated the results obtained from sample data across the wider assessment period.

85. RW2 further accepted that the DMS does not verify payment of OTT tax and that OVA payment records were not utilised during the DMS analysis. He also acknowledged that one subscriber may pay the OTT tax on behalf of another subscriber and that the Respondent's methodology focused on access rather than on tracing individual payment sources. He further accepted that anomalies existed within portions of the dataset, including truncated IMSIs. However, he testified that such anomalies represented a very small proportion of the overall dataset and did not materially affect the assessment.

86. In re-examination, RW2 reiterated that the assessment was based on information obtained directly from the Applicant's network, analysed using the DMS methodology and subjected to audit and reconciliation procedures before the assessment was issued.

V. Submissions of the Applicant

Whether the Respondent's assessment was contrary to the Excise Duty (Amendment) Act, 2018

87. The Applicant submitted that the additional assessment of UGX 33,911,117,000 lacked both a statutory and factual foundation under paragraph 13(b) of the Second Schedule to the Excise Duty (Amendment) Act, 2018. It argued that the Respondent assessed tax on transactions that did not constitute taxable access to Over-the-Top (OTT) services as contemplated by the law.

88. According to the Applicant, liability to OTT tax arose only when three elements were present simultaneously: an identifiable user, a specified day, and actual access to an OTT service. The Applicant submitted that the phrase "Ushs 200 per user per day of access" required proof of a particular user accessing an OTT service on a particular day. The Applicant relied on section 2 of the Excise Duty (Amendment) Act, 2018, which defined "over-the-top services" as the transmission or receipt of voice or messages over an internet protocol network and included access to a virtual private network. It submitted that the taxable event under the statute was therefore the actual transmission or receipt of voice or messages over an internet protocol network and not merely the generation of network traffic.

89. The Applicant argued that the Respondent's methodology impermissibly substituted the statutory definition of access with a technical assumption that the generation of more than one kilobyte (1KB) of traffic constituted access to an OTT service. According to the Applicant, neither the Act nor any subsidiary legislation prescribed a 1KB threshold, and the Respondent thereby introduced a new taxable event that had not been enacted by Parliament.

90. The Applicant further submitted that Article 152(1) of the Constitution prohibits the imposition of tax except under the authority of an Act of Parliament. It argued that the Respondent's adoption of a 1KB threshold amounted to the creation of a new tax criterion through administrative action rather than legislation.

91. In support of this proposition, the Applicant cited ***Cape Brandy Syndicate v IRC [1921] 1 KB 64***, where it was held that there is no room for intendment in taxing statutes and nothing is to be read in or implied. The Applicant further cited ***URA v Airtel Uganda Limited (Civil Appeal No. 032 of 2020)*** and ***URA v Kajura (Civil Appeal No. 09 of 2015)***, where the courts emphasised that tax

liability must arise from the express words of the statute and not from implication or administrative interpretation.

92. The Applicant also submitted that even following the purposive approach to statutory interpretation discussed in ***Nile Breweries Limited v Uganda Revenue Authority (Civil Appeal No. 0014 of 2022)***, Parliament intended to tax actual use of OTT services and not the mere movement of data packets within a telecommunications network.

93. The Applicant challenged the additional assessment of UGX 33,911,117,000 on the ground that it lacked both a statutory and factual basis under **Paragraph 13(b) of the Second Schedule to the Excise Duty Act, 2018 (as amended)**. The Applicant maintained that the Respondent assessed tax on transactions that did not constitute taxable access to Over-the-Top (OTT) services as contemplated by the law.

94. The Applicant submitted that the Respondent's methodology was fundamentally flawed because it relied on information captured from the GTP Region of the Applicant's telecommunications network rather than the Gi Region, where actual internet access occurs. According to the Applicant, the GTP Region captures signalling traffic, attempted communications, retransmissions and network activity generated before access-control mechanisms are applied.

95. By contrast, the Gi Region is situated after the Applicant's Policy and Charging Rules Function (PCRF) and Policy Control and Enforcement Function (PCEF), where actual internet access and OTT communication occur. The Applicant argued that successful OTT access can occur only after a subscriber has paid the prescribed tax and been authorised by the PCRF. It is therefore submitted that information captured before the operation of the PCRF cannot reliably establish taxable access.

96. The Applicant relied on the evidence of AW2 and the demonstration conducted before the Tribunal. It is submitted that the demonstration showed that a subscriber who had not paid OTT tax could generate traffic in excess of 1KB while attempting to access WhatsApp, but remain incapable of transmitting or receiving any message because access had been blocked by the PCRF. According to the Applicant, the demonstration established that data traffic exceeding 1KB does not necessarily indicate successful OTT access and that the Respondent's methodology conflated attempted access with actual access. The Applicant therefore argued that the Respondent's probe captured unsegregated traffic, including blocked attempts, signalling traffic and other non-taxable communications, and failed to distinguish such traffic from actual OTT access.

97. The Applicant further submitted that the Respondent's own witness acknowledged that the monitoring probe was installed within the GTP Region and that the system did not independently verify whether a subscriber ultimately accessed an OTT service.

Whether the Respondent's Methodology Was Consistent with the Agreed Framework for Implementation of OTT Tax

98. The Applicant submitted that at the commencement of the OTT regime, stakeholders, including the Uganda Communications Commission and telecommunications operators, agreed on the operational framework for implementation of the tax. It relied on the minutes and records of a meeting held on 27 June 2018, at which it was agreed that access to OTT services would be blocked with effect from 1st July 2018 and granted only upon payment of the prescribed OTT tax.

99. According to the Applicant, it implemented the agreed framework by deploying a Policy and Charging Rules Function (PCRF) integrated with the Online Virtual Account (OVA) platform. The Applicant submitted that the PCRF

verified OTT tax payments and denied access to subscribers who had not paid, permitting access only after payment was confirmed.

100. The Applicant argued that the Respondent's methodology ignored the agreed implementation framework and instead relied on data captured before the PCRF verification process. It therefore contended that the Respondent's methodology was inconsistent with the operational arrangements adopted by stakeholders for administration of the OTT tax and was incapable of reliably determining whether a subscriber had actually obtained access to an OTT service.

Whether the Respondent failed to reconcile DMS Data with OVA Payment Records

101. The Applicant submitted that the Online Virtual Account (OVA) platform was specifically established to facilitate the collection and administration of OTT tax and the recording of payments in real time. According to the Applicant, both parties had access to the OVA system and could therefore verify whether OTT tax had been paid by a particular subscriber. The Applicant argued that despite having access to the OVA records, the Respondent failed to reconcile the alleged OTT accesses identified through the Data Monitoring System with the corresponding payment records maintained in the OVA.

102. The Applicant particularly cited IMSI 64110100330202015, which the Respondent allegedly identified as non-compliant. The Applicant submitted that a review of the OVA records showed that OTT tax had in fact been paid in respect of that subscriber during the relevant period. The Applicant therefore argued that the Respondent's failure to reconcile DMS data with OVA payment records rendered the assessment unreliable and demonstrated that the methodology was incapable of accurately identifying non-compliant subscribers.

103. The Applicant submitted that the Respondent failed to identify the specific taxable transactions giving rise to the assessment. According to the Applicant, the statutory structure of the OTT tax required proof of an identifiable user, a particular day of access and actual access to an OTT service. It is therefore argued that any lawful assessment required identification of the relevant subscriber, the date on which access occurred and evidence that the subscriber accessed an OTT service without payment of the prescribed tax.

104. The Applicant contended that the Respondent did not produce evidence showing that particular subscribers accessed OTT services, transmitted or received messages over an internet protocol network, and failed to pay OTT tax in respect of those accesses. It argued that the Respondent instead relied on aggregate datasets and assumptions derived from network traffic.

105. According to the Applicant, the only lawful basis for the assessment would have been evidence demonstrating that a particular customer accessed an OTT service on a particular day and had not paid the applicable tax for that access. The Applicant, therefore, maintained that the Respondent failed to establish the factual basis of the alleged understatement.

Whether the Respondent relied on reliable and verifiable data

106. The Applicant submitted that the Respondent failed to disclose the complete datasets, business rules, analytical assumptions, and computations used to generate the assessment. According to the Applicant, the Respondent did not identify specific subscribers who allegedly accessed OTT services without payment of tax, nor did it disclose sufficient information to enable the Applicant to independently verify the assessment.

107. The Applicant further challenged the integrity of the technical data relied upon by the Respondent. It submitted that some of the IP addresses used to identify OTT traffic were subsequently verified with Meta Platforms Inc. and found not

to belong to Facebook or WhatsApp. The Applicant also submitted that certain IMSIs appearing in the Respondent's datasets were incomplete or inconsistent with the Applicant's network architecture and numbering structure.

108. The Applicant further submitted that the Respondent's datasets included traffic associated with virtual private networks (VPNs), contrary to the agreed implementation parameters applicable during the operation of the OTT regime. According to the Applicant, the inclusion of VPN-related traffic among the accesses relied upon by the Respondent further demonstrated that the assessment was founded on inaccurate and unfiltered data incapable of reliably establishing taxable OTT access.

109. According to the Applicant, these anomalies demonstrated that the Respondent's datasets were unreliable and incapable of supporting the impugned assessment.

The 5-day data sample

110. The Applicant further challenged the basis upon which the Respondent derived the impugned assessment. It submitted that following a series of reconciliations and engagements between the parties, the Respondent agreed to analyse a sample comprising five days of data covering the period from 1st May 2021 to 5th May 2021. According to the Applicant, the parties remained in disagreement regarding the conclusions drawn from that sample.

111. The Applicant argued that, notwithstanding the limited nature of the sample period, the Respondent proceeded to derive conclusions regarding alleged under-declarations for the entire assessment period extending from April 2020 to June 2021. It submitted that the Respondent's methodology therefore rested on extrapolations, assumptions and estimates rather than verified instances of taxable access by identifiable subscribers.

112. According to the Applicant, the Respondent failed to demonstrate that the sample period was representative of the entire assessment period or that the assumptions derived from the sample could reliably be applied to all transactions during the relevant period. The Applicant, therefore, maintained that the resulting assessment lacked a proper factual foundation.

Whether the Respondent's methodology violated the principles of certainty, legality and non-Retrospectivity

113. The Applicant submitted that the Respondent's reliance on the 1KB threshold offended the principles of certainty, legality and non-retrospectivity in taxation. It argued that the threshold was never communicated to telecommunications operators during the OTT tax regime and only emerged during the audit process, after the tax had already been repealed.

114. The Applicant relied on **Farid Meghani v URA (Civil Appeal No. 6 of 2021)** for the proposition that certainty is a cornerstone of the rule of law and that ambiguities in tax legislation should be resolved in favour of the taxpayer. It further relied on **Britania Allied Industries v Uganda Revenue Authority (HCCA No. HCT-00-CC-CA-042-2023)**, where retrospective tax demands based on a later reclassification were held to result in conspicuous unfairness.

115. They also cited ***National Social Security Fund v Uganda Revenue Authority (Civil Appeal No. 29 of 2022)***, where the Court of Appeal held that a public authority's change of position ordinarily takes effect prospectively. The Applicant therefore submitted that even if the Respondent were entitled to adopt a new methodology, which it denied, that methodology could not lawfully be applied retrospectively to transactions that occurred before the methodology was disclosed.

Whether the IP Addresses Relied Upon by the Respondent Properly Identified OTT Services

116. The Applicant further challenged the reliability of the IP addresses that the Respondent relied upon to identify OTT traffic. It submitted that during the audit and reconciliation exercises, the Respondent provided a list of IP addresses allegedly associated with OTT services, including Facebook and WhatsApp. According to the Applicant, those IP addresses were subsequently submitted to Meta Platforms Inc., the parent company of Facebook and WhatsApp, for verification. The Applicant submitted that Meta confirmed that some of the IP addresses relied upon by the Respondent did not belong to Facebook or WhatsApp during the relevant period. The Applicant contended that the Respondent did not controvert this evidence.

117. The Applicant therefore argued that the Respondent relied on inaccurate or improperly classified traffic in identifying OTT accesses and that such inaccuracies undermined the integrity and reliability of the assessment methodology.

Whether the Applicant Discharged the Burden of Proof

118. The Applicant acknowledged that section 19 of the Tax Appeals Tribunal Act and section 28 of the Tax Procedures Code Act place the burden upon an applicant to prove that an assessment is excessive or erroneous. It also relied on section 103 of the Evidence Act. The Applicant nevertheless submitted that it had discharged that burden by producing documentary evidence, expert testimony, technical demonstrations, payment records and network architecture evidence showing that the assessment was founded on erroneous assumptions and an unlawful methodology.

119. The Applicant argued that once it had established a prima facie case, the evidential burden shifted to the Respondent to justify the assessment. In support of this proposition, it relied on ***Steel Corporation of East Africa v***

URA (HCCA No. HCT-OO-CC-CA-O-2010), J.K. Patel v Spear Motors Ltd (Civil Appeal No. 4 of 1991), URA v K-Files Ltd (Civil Appeal No. 0028 of 2022), Kamo Enterprises Ltd v Krystaline Salt Ltd (Civil Appeal No. 8 of 2018), *and* ***URA v Balondemu David (Civil Appeal No. 0002 of 2023).*** According to the Applicant, the Respondent failed to rebut the evidence adduced and therefore failed to establish the correctness of the assessment.

Reliefs sought

120. The Applicant accordingly prayed that the Application be allowed, that the additional assessment and objection decision be set aside, that the statutory deposit of 30 per cent be refunded, and that costs be awarded in its favour. In support of its claim for costs, the Applicant relied on section 22 of the Tax Appeals Tribunal Act, section 27 of the Civil Procedure Act, and the decisions in **Candiru v Amandua & 2 Ors (Civil Suit 19 of 2014) [2017] UGHCCD 139 (27 October 2017), Hajji Musa Hasahya v Owori & Co. Advocates (HCCA No. 71 of 2011), U.T.C. v Outa [1985] (UHCB 27),** and **Premchand Raichand Ltd v Quarry Services of East Africa Ltd and Others (No. 3) [1972] EALR 162**

VI. Submissions of the Respondent

121. The Respondent opposed the Application and maintained that the additional Local Excise Duty assessment of UGX 33,911,117,000 was lawfully issued and correctly reflected the Applicant's liability under the Excise Duty (Amendment) Act, 2018. The Respondent contended that both the legal and technical foundations of the assessment were sound and that the Applicant had failed to discharge the statutory burden required to impugn the assessment.

122. The Respondent submitted that the law places the burden of proving that a tax assessment is excessive or erroneous squarely upon the taxpayer. Reliance was placed on section 19 of the Tax Appeals Tribunal Act and section 28 of

the Tax Procedures Code Act, which require an applicant challenging a tax decision to demonstrate that the assessment is incorrect or that the decision ought to have been made differently.

123. The Respondent further relied on Williamson Diamonds Ltd v Commissioner General (4 TTLR 167), wherein it was held that the burden of disproving an assessment rests upon the taxpayer and does not shift to the revenue authority merely because the taxpayer disputes the assessment. Accordingly, the Respondent argued that throughout these proceedings, the Applicant bore the obligation of demonstrating that the assessment lacked a factual or legal basis.

124. The Respondent submitted that the Applicant's liability arose from its provision of access to OTT services within the meaning and purpose of the Excise Duty (Amendment) Act, 2018.

125. While acknowledging that the Act did not expressly define the term "access," the Respondent argued that the ordinary and contextual meaning of the term should be adopted. Reliance was placed on the decision of Stephen Mubiru J. in ***Nile Breweries Limited v URA & 2 Others (Civil Appeal No. 14 of 2022)***, wherein the Court emphasised that where legislation does not define a particular term, courts should interpret the term according to its ordinary meaning within the context and purpose of the statute.

126. The Respondent also referred to Black's Law Dictionary (11th Edition), which defines access as a "right, opportunity, or ability to enter, approach, pass to and from, or communicate with." Based on this definition, the Respondent submitted that a subscriber acquired access once the telecommunications network provided the technical capability and opportunity to connect to an identified OTT service. In its view, actual transmission or receipt of messages was not the sole determinant of access; rather, the enabling of connectivity constituted the taxable event contemplated by the legislation.

127. The Respondent therefore contended that the Applicant's interpretation of access was unduly restrictive and inconsistent with both the purpose of the legislation and the ordinary meaning of the term. The Respondent defended the methodology used to generate the assessment and maintained that the Data Monitoring System (DMS) and Telecom Information Management System (TIMS) were lawfully deployed for revenue assurance and the verification of returns submitted by telecommunications operators.

128. The Respondent submitted that the GPRS Tunnelling Protocol (GTP) region constituted the most appropriate point within the telecommunications network for monitoring subscriber activity relevant to OTT taxation.

129. According to the Respondent, the Gi interface was unsuitable for revenue assurance purposes because it primarily facilitated internet traffic routing and lacked subscriber-specific identifiers necessary for accurate tax verification. It was further argued that the Gi interface employed Network Address Translation (NAT), which obscured subscriber identities and rendered direct attribution of traffic to particular users difficult.

130. By contrast, the Respondent submitted that the GTP region preserved critical subscriber identifiers such as the International Mobile Subscriber Identity (IMSI), Mobile Station International Subscriber Directory Number (MSISDN), and PDP Context information. These identifiers enabled traffic records to be associated with specific subscribers, thereby facilitating accurate computation of OTT tax liabilities.

131. The Respondent further noted that the Applicant had previously cooperated in providing access to the GTP region and had not objected to its use during the implementation of the OTT tax regime.

132. The Respondent rejected the Applicant's assertion that the assessment was based on raw or unprocessed traffic data. It submitted that the information collected from the GTP region underwent extensive processing and validation before being incorporated into the assessment.

133. The Respondent explained that a filtering methodology had been developed and communicated to telecommunications operators, including the Applicant, in June 2018. This methodology ensured that multiple accesses by the same subscriber within a twenty-four-hour period were consolidated and counted only once, thereby preventing duplication and overstatement of liability.

134. With respect to the disputed 1KB threshold, the Respondent submitted that the parameter was introduced as a technical validation measure to distinguish successful access from failed or incomplete attempts. According to the Respondent, traffic records involving less than 1KB of data were excluded from computation because they were likely indicative of unsuccessful connection attempts or network signalling activity.

135. The Respondent therefore maintained that the threshold enhanced rather than distorted the accuracy of the assessment and was necessary to ensure that only genuine instances of OTT access were captured.

136. The Respondent denied allegations that it had failed to disclose the information upon which the assessment was based. It submitted that during the objection review process, it provided the Applicant with five days of raw sample data containing subscriber identifiers and associated IP addresses. The Respondent argued that, despite receiving this information, the Applicant failed to provide corresponding network data to disprove the Respondent's findings or to demonstrate errors in the computation.

137. The Respondent further contended that the Applicant's reliance on Online Virtual Account (OVA) records was misplaced. While acknowledging that the OVA served as a useful mechanism for recording aggregate tax collections, the Respondent submitted that it lacked the network-level granularity required to identify individual subscriber access events. Consequently, the Respondent argued that OVA records could not conclusively establish whether particular users had accessed OTT services without payment of the prescribed tax.

138. The Respondent also addressed concerns regarding Virtual Private Networks (VPNs), clarifying that such traffic was segregated by the system's processing logic and was not included in the assessed figures.

139. The Respondent maintained that the assessment was supported by substantial documentary, technical, and testimonial evidence presented before the Tribunal. It relied on witness testimony and video demonstrations tendered as Respondent Exhibits REX 7, REX 8, REX 9, and REX 10, which, in its view, demonstrated the functionality of the monitoring systems, the integrity of the processing methodology, and the accuracy of the resulting computations. The Respondent, therefore, contended that the Applicant had failed to establish any material error in either the legal interpretation adopted or the technical methodology applied in arriving at the assessment.

140. In light of the foregoing, the Respondent prayed that the Tribunal dismiss the Application with costs and uphold the assessment in its entirety. Specifically, the Respondent sought orders that the Application be dismissed, the Applicant be held liable for the assessed Local Excise Duty amounting to UGX 33,911,117,000, and the costs of the Application be awarded to the Respondent.

VII. Submissions of the Applicant in rejoinder

141. In rejoinder, the Applicant maintained that the Respondent's submissions did not cure the fundamental legal, evidential, and technical defects in the assessment. The Applicant reiterated that the assessment of UGX 33,911,117,000 was founded on an erroneous interpretation of the Excise Duty Act, an unreliable technical methodology, and speculative extrapolations unsupported by verifiable taxpayer-specific data.

142. The Applicant challenged the probative value of the Respondent's video demonstrations, contending that they did not establish actual taxable access to OTT services.

143. With respect to Exhibit REX 7, the Applicant submitted that the demonstration merely showed data capture within the GTP region, which occurred before a subscriber obtained actual access to the internet. The Applicant argued that such data could include signalling traffic, failed attempts, and blocked sessions, and therefore could not, without more, prove actual access to OTT services.

144. The Applicant further pointed out that the timestamps displayed in the video referred to the year 2025, whereas the assessment related to an earlier tax period. In the Applicant's view, this discrepancy materially undermined the relevance and reliability of the exhibit.

145. Regarding Exhibit REX 8, the Applicant submitted that the demonstration was internally inconsistent because it reflected zero blocked OTT accesses between 1 May and 5 May 2020. The Applicant argued that this result was practically implausible given the operation of the PCRF blocking mechanism and demonstrated that the Respondent's probe in the GTP region was incapable of identifying blocked attempts. The Applicant, therefore, contended

that the Respondent's system could not reliably distinguish taxable access from non-taxable attempted access.

146. In relation to Exhibit REX 10, the Applicant challenged the Respondent's claim that its system prevented duplicate counting. The Applicant submitted that the demonstration showed manual inputs and workings in an Excel sheet rather than an automated, auditable process capable of processing millions of alleged access events. The Applicant argued that such manual intervention rendered the methodology error-prone and fell short of the evidential standard required to support an assessment of this magnitude.

147. The Applicant reiterated that while the initial burden lay on it under section 19 of the Tax Appeals Tribunal Act and section 28 of the Tax Procedures Code Act, that burden had been discharged through credible technical and documentary evidence demonstrating material defects in the assessment.

148. The Applicant relied on ***Safe Gears Limited v URA (TAT Application No. 91 of 2024)*** for the proposition that once a taxpayer adduces credible evidence challenging the basis of an assessment, the evidential burden shifts to the tax authority to justify the assessment. The Applicant argued that this principle was particularly applicable where the Respondent sought to rely on a methodology not expressly prescribed by statute and where the tax authority departed from ordinarily verifiable records.

149. The Applicant submitted that the Respondent failed to discharge this evidential burden. In particular, the Respondent did not identify specific non-compliant subscribers, did not reconcile the alleged access data with the Online Virtual Account, and did not provide a complete and verifiable audit trail showing how the assessed amount was computed.

150. The Applicant further submitted that the assessment violated fundamental principles governing taxation. First, the Applicant argued that the 1KB threshold offended the canon of legality and Article 152(1) of the Constitution, which requires taxation to be imposed only under authority of an Act of Parliament. The Applicant maintained that neither the Excise Duty Act nor any subsidiary legislation authorized the Respondent to create a 1KB threshold as a determinant of taxable access.

151. Secondly, the Applicant contended that the assessment offended the principle of certainty because the Respondent's methodology was inconsistent, unclear, and incapable of independent verification.Thirdly, the Applicant submitted that the assessment lacked transparency because it was based on incomplete data, disputed demonstrations, and processing logic that was neither fully disclosed nor reconciled with the statutory payment records.

152. The Applicant relied on Sande Pande Ndimwibo v URA (Civil Suit No. 424 of 2012) for the proposition that tax assessments must be strictly grounded in legislation and cannot be founded on administrative interpretation, internal policy, or technical assumptions not anchored in an Act of Parliament.

153. The Applicant maintained that the Respondent's methodology conflated subscriber identification with actual access to OTT services. While the GTP region may contain subscriber identifiers such as IMSI and MSISDN, the Applicant argued that such identifiers did not prove that a subscriber successfully accessed an OTT service. According to the Applicant, actual access could only be confirmed after the PCRF system had permitted the subscriber to proceed beyond the blocking mechanism and access the internet through the Gi region.

154. The Applicant further submitted that the Respondent's filtration process was not shown to be technically reliable. In particular, the Applicant argued that the

Respondent failed to account for subscribers who paid for weekly or monthly OTT bundles, or subscribers whose OTT tax obligations were settled by third parties. The Applicant contended that these omissions created a real risk that compliant subscribers were wrongly treated as non-compliant.

155. The Applicant also challenged the Respondent's reliance on a disputed five-day sample to extrapolate liability over a fifteen-month period. It submitted that such extrapolation was statistically unreliable, legally unsustainable, and arbitrary, particularly where the underlying sample itself was contested and had not been reconciled with payment records.

156. The Applicant submitted that the Respondent's data suffered from material integrity concerns. It pointed to truncated and unknown IMSIs which did not conform to the Applicant's 15-digit network nomenclature and argued that such defects compromised the reliability of the dataset as a whole.

157. The Applicant also disputed the Respondent's assertion that VPN traffic had been excluded from the assessment. It is submitted that references to VPN traffic remained in the Respondent's processed data, suggesting that such traffic may have been included in the computation and thereby inflated the assessment.

158. Most significantly, the Applicant emphasised the Respondent's failure to reconcile its probed data with the Online Virtual Account. The Applicant submitted that the OVA was the agreed and accessible platform for verifying OTT tax payments. It relied on a specific IMSI, which the Respondent had treated as non-compliant, yet the OVA records showed that the subscriber had paid for daily and weekly OTT bundles. The Applicant argued that this example demonstrated a fundamental flaw in the Respondent's methodology and cast doubt on the reliability of the entire assessment.

159. The Applicant therefore maintained that the Respondent had failed to justify the assessment. It submitted that the assessment was based on unproven assumptions, technically unreliable data capture, inadequate filtration, and speculative extrapolation. The Applicant accordingly prayed that the Tribunal find the assessment of UGX 33,911,117,000 unlawful, set aside the objection decision, order a refund of the statutory deposit, and award the Applicant costs of the Application.

VIII. The Determination

160. We have carefully considered the pleadings, witness statements, oral and documentary evidence, electronic demonstrations, written submissions of Counsel, and the authorities cited by the parties. The principal issue for determination is whether the Respondent lawfully and properly assessed the Applicant to additional Local Excise Duty on Over-the-Top services for the period April 2020 to June 2021 in the sum of Shs. 33,911,117,000.

161. The assessment arose from the Respondent's comparison between OTT accesses declared by the Applicant in its Local Excise Duty returns and accesses allegedly identified through the Government's Data Monitoring System, also referred to in the proceedings as DMS or TIMS, operated by the Global Voice Group, a third party contractor. According to the Respondent, the system identified 308,793,188 unique OTT accesses, whereas the Applicant declared 139,237,602 accesses. The difference of 169,555,586 accesses formed the basis of the impugned assessment.

162. The Applicant disputed the assessment on both legal and technical grounds. It contended that the assessment was founded on a methodology unsupported by statute, based on data captured at an inappropriate point in the network, and incapable of proving actual taxable access by identifiable users who had not paid OTT tax. The Respondent, on the other hand, maintained that the assessment was based on independent data captured from the Applicant's

network, processed through the Data Management System, and subjected to audit and reconciliation processes. The Respondent argued that the Applicant had failed to demonstrate that the assessment was excessive or erroneous.

163. The determination of this issue therefore requires the Tribunal to consider the statutory basis of OTT tax, the meaning of taxable access, the reliability of the Respondent's methodology, the sufficiency of disclosure, the evidential value of the technical data relied upon, and the burden of proof.

The legal framework

164. Article 152(1) of the Constitution provides that no tax shall be imposed except under the authority of an Act of Parliament. This constitutional provision embodies the principle of legality in taxation. A tax liability must be grounded in clear statutory authority and cannot arise merely from administrative practice, inference, convenience, or technical assumption.

165. The relevant statutory provision for purposes of excise duty on OTT services was paragraph 13(b) of the Second Schedule to the Excise Duty (Amendment) Act, 2018 (since repealed). It imposed excise duty on "Over the Top services" at the rate of Shs. 200 per user per day of access. Further, Section 2 of the Excise Duty (Amendment) Act, 2018 defined "over-the-top services" as the transmission or receipt of voice or messages over the internet protocol network and included access to a virtual private network.

166. The statutory formulation therefore contains three material elements, namely:

(i) First, there must be a user.

(ii) Secondly, there must be a relevant day or period of access.

(iii) Thirdly, there must be access to an OTT service, meaning transmission or receipt of voice or messages over an internet protocol network, or access to a virtual private network.

167. The Tribunal recognizes the general principle stated in ***Cape Brandy Syndicate v IRC [1921] 1 KB 64*** that in a taxing statute, one must look merely at what is clearly said, and there is no room for intendment. Nothing is to be read in or implied. The same principle has consistently been applied in Uganda including in ***Uganda Revenue Authority v Airtel Uganda Limited, Civil Appeal No. 032 of 2020, and Uganda Revenue Authority v Kajura, Civil Appeal No. 09 of 2015***. In ***Commissioner General, Uganda Revenue Authority v Kajura [Supreme Court of Uganda]***, the Supreme Court reiterated that a taxing statute must be interpreted according to the language employed by Parliament and that liability cannot be imposed by implication or administrative convenience. Where ambiguity exists, the court's task is to ascertain Parliament's intention from the statutory text rather than from assumptions as to the desirability of collecting revenue in a particular manner. These authorities reinforce the principle that the Respondent's methodology must correspond with the statutory charging event and cannot itself define the scope of the tax.

168. The Tribunal also takes guidance from ***Farid Meghani v Uganda Revenue Authority, Civil Appeal No. 6 of 2021***, on the requirement of certainty in taxation; ***Britania Allied Industries v Uganda Revenue Authority, HCCA No. HCT-00-CC-CA-042-2023***, on unfairness arising from retrospective administrative positions; and ***National Social Security Fund v Uganda Revenue Authority, Civil Appeal No. 29 of 2022,*** on the prospective effect of changes in interpretation by a public authority.

169. The Tribunal further considers ***Nile Breweries Limited v Uganda Revenue Authority, Civil Appeal No. 0014 of 2022***. That decision recognises that a purposive approach may be adopted where appropriate. Even under a purposive approach, the purpose must be derived from the statute and not from administrative convenience.

Burden of proof

170. On burden of proof, section 19 of the Tax Appeals Tribunal Act places the burden on an applicant to prove that a taxation decision is excessive or erroneous. Section 28 of the Tax Procedures Code Act is to similar effect. The Tribunal therefore agrees with the Respondent's submission that the taxpayer bears the legal burden of disproving an assessment. A taxpayer cannot succeed by merely denying liability or by pointing to administrative imperfections that do not affect the correctness of the assessment.

171. However, the statutory burden does not require a taxpayer to prove the impossible. Where an applicant adduces credible evidence showing material legal, factual or technical defects in the methodology upon which an assessment is founded, the Tribunal must evaluate whether the assessment remains sustainable on the totality of the evidence before it. This inquiry does not reverse the burden imposed by section 19 of the Tax Appeals Tribunal Act. Rather, it reflects the Tribunal's obligation to determine whether the Applicant has demonstrated that the assessment is excessive or that the taxation decision ought to have been made differently.

172. We are guided by the decisions in ***Steel Corporation of East Africa v Uganda Revenue Authority, HCT-00-CC-CA-0-2010, Uganda Revenue Authority v K-Files Ltd, Civil Appeal No. 28 of 2022*** and ***Uganda Revenue Authority v Balondemu David, High Court Civil Appeal No. 0002 of 2023,*** which recognise the distinction between the legal burden of proof and the evidential burden. The legal burden imposed by section 19 of the Tax Appeals Tribunal Act and section 28 of the Tax Procedures Code Act remains throughout upon the Applicant to demonstrate that the assessment is excessive or ought not to have been made. However, where the Applicant adduces credible technical, documentary and oral evidence that materially challenges the factual or legal basis of the assessment, the Respondent bears the evidential burden of answering that evidence if the assessment is to remain persuasive. This does not amount to a reversal of the statutory burden of proof;

rather, it reflects the ordinary operation of the evidential burden in adversarial proceedings, requiring the Tribunal to evaluate the entirety of the evidence in determining whether the assessment has been justified.

173. The Tribunal's task is not to determine whether the Respondent's methodology was theoretically capable of identifying taxable OTT access, nor whether an alternative methodology might have been preferable. The question before the Tribunal is narrower: whether, on the evidence presented in these proceedings, the methodology employed provided a sufficiently reliable basis for the assessment under challenge. The Tribunal must therefore evaluate not the abstract validity of the Respondent's system, but the reliability of its application to the assessment period and taxpayers in issue.

Inadequacy of the Excise Duty Act

174. The difficulty in this case arises from the fact that the Act imposed tax "per user per day of access" but did not define with precision what constituted "access" for purposes of a packet-switched telecommunications network. The legislation did not specify whether access occurred when a subscriber initiated a request to an OTT platform, when traffic associated with an OTT application traversed a particular network interface, when a specified volume of data was exchanged, when a particular data-volume threshold was crossed, when a connection was successfully established, when the subscriber successfully transmitted or received a message through the OTT service, or indeed some other objectively verifiable network event.

175. Nor did the Act prescribe the technical indicators of access, by which access was to be measured, the network point/location at which access was to be determined, the treatment of unsuccessful connection attempts, retransmissions, signalling traffic, VPN traffic, third-party payments, weekly or monthly bundles, or the reconciliation mechanism between network monitoring

data and payment data. The Act did not define "a day." Was it a calendar day or a 24 hour period?

176. In a simple retail excise context, such omissions may not create serious difficulty. In the present context, however, the tax was imposed on highly complex digital network behaviour. The absence of legislative precision created real uncertainty in implementation and enforcement. These were matters of fundamental importance to the administration of the tax, yet they were left unresolved by the legislation itself. The Tribunal does not suggest that Parliament was required to prescribe network-engineering specifications or detailed telecommunications protocols. However, where liability depended upon identifying a particular technological event within a complex digital environment, the absence of objective statutory indicators of access created uncertainty as to the precise event intended to attract tax.

Operationalisation of the EDA through stakeholder engagements

177. The Tribunal notes that shortly after enactment of the tax and prior to its implementation on 1 July 2018, stakeholders comprising the Uganda Revenue Authority, the Uganda Communications Commission (UCC), and telecommunications operators, including the Applicant, convened a series of meetings to discuss the practical modalities for implementation of the tax. The evidence of AW1, supported by Exhibits A1 and A2, was that these engagements culminated in an agreed operational framework under which subscribers who had not paid the OTT tax would be denied access to OTT services, while access would be granted only upon payment of the prescribed tax. The Tribunal further notes that Online Virtual Accounts (OVAs) were established to facilitate remittance and reconciliation of OTT tax collections and that operators were permitted to deploy technological solutions capable of enforcing the agreed framework.

178. The Tribunal considers this evidence significant for two reasons. First, it demonstrates that the principal stakeholders responsible for implementing the tax recognised the need to develop administrative and technical mechanisms to operationalise the charging provision. Secondly, it demonstrates that the concept of "access" was not self-evident from the statutory language and required practical interpretation before implementation could occur.

179. In the Tribunal's view, the stakeholder agreement that unpaid subscribers would be blocked from accessing OTT services is particularly revealing. While such an agreement could not amend the statute or create tax liability where none existed, it provides important context regarding how the parties charged with implementing the legislation understood the taxable event. The implementation framework proceeded on the premise that tax became payable in connection with successful access to OTT services and that non-paying subscribers would be prevented from obtaining such access. It did not proceed on the premise that every attempted access, signalling exchange, or packet of data associated with an OTT application would itself constitute a taxable event.

180. The Tribunal is mindful that administrative agreements cannot override statutory language. However, where a charging provision is ambiguous or technically incomplete, contemporaneous implementation arrangements involving the regulator, the tax authority and regulated operators may provide useful context in understanding the practical operation of the statutory scheme. The Tribunal has not treated the consultations held between the Uganda Communications Commission, the Respondent and telecommunications operators as instruments capable of amending or supplementing the Act, or of creating tax liabilities not imposed by Parliament. Their significance lies in the fact that they formed part of the implementation of the newly enacted levy and illustrate the practical challenges encountered in identifying the technological events intended to attract the tax. Accordingly, the Tribunal relies on those engagements only as contemporaneous evidence of how the regime was

implemented in practice, and not as a basis for displacing or modifying the ordinary meaning of the statutory language.

181. We find persuasive the decision in ***R v Inland Revenue Commissioners, ex parte National Federation of Self-Employed and Small Businesses Ltd [1982] AC 617***, where the House of Lords reaffirmed that public authorities derive their powers from statute and cannot enlarge or alter statutory obligations through administrative practice. Those principles reinforce the Tribunal's approach that stakeholder engagements may illuminate factual context but cannot determine the legal scope of the charging provision.

182. The uncertainty inherent in the charging provision is not merely a matter of drafting. It is central to the present dispute. The Applicant contends that taxable access occurred only after its PCRF system permitted the user to reach OTT services. The Respondent contends that subscriber-identifiable traffic captured within the GTP environment, once processed through its filters in the DMS methodology, was sufficient to evidence taxable access. The Tribunal finds that the existence of these competing interpretations illustrates the absence of clear statutory guidance on the precise technical event that Parliament intended to tax.

183. In tax law, such uncertainty must be approached with caution. The Tribunal cannot enlarge the scope of a charging provision through administrative practice, technical assumptions or post facto interpretations. As was stated in ***Cape Brandy Syndicate v IRC [1921] 2 KB 6***4, and reaffirmed in subsequent Ugandan authorities, a taxpayer can only be taxed upon clear words of Parliament. Where liability depends upon identifying a specific taxable event and Parliament has not prescribed objective criteria for identifying that event, the Tribunal must be satisfied that the administrative methodology relied upon remains faithful to the statutory language and does not enlarge the charge imposed by Parliament.

184. The Tribunal finds that the Respondent was entitled to adopt technical tools for audit and verification. However, those tools could not create a taxable event different from, or broader than, the one enacted by Parliament. The uncertainty in the charging provision required the Respondent to be especially careful to demonstrate, by clear and reliable evidence, that the activities captured by its monitoring system and its resultant assessment corresponded to the statutory taxable event, namely access by a user to an OTT service. It was not sufficient merely to show that data associated with a subscriber moved through a particular part of the telecommunications network.

185. The Tribunal must therefore examine whether the evidence relied upon by the Respondent established a sufficiently reliable nexus between the monitored activity and the taxable event contemplated by the Act. The question is not whether the Respondent was required to prove the assessment afresh, but whether the Applicant has demonstrated that the methodology employed was insufficiently reliable to sustain the assessment.

186. The Tribunal has also considered the Respondent's broader submission that the OTT tax was enacted as a revenue measure intended to capture widespread use of internet-based communication platforms. That proposition may be accepted as a matter of legislative purpose. However, the language of the Act ought to reflect the intended legislative purpose and courts will only depart from the language chosen by Parliament in exceptional circumstances, e.g, where the language results in absurdity, which is not the case here. Therefore, the obligation of the Tribunal is to identify the taxable event enacted by Parliament and determine whether the impugned assessment corresponds to that event.

Meaning of "Access" in the context of the OTT Tax

187. The Respondent urged the Tribunal to adopt the ordinary meaning of the word "access", relying on Black's Law Dictionary and ***Nile Breweries Limited v***

Uganda Revenue Authority & 2 Others, Civil Appeal No. 14 of 2022. In that decision, the Court observed:

"The panopoly of tax legislation is notoriously complex and can be difficult to interpret. The majority of statutes have definition sections that explain the specific meaning of words or phrases used within that statute, to avoid confusion, reduce repetition, and ensure clarity in their application and in order to ensure that specific terms are understood and applied consistently throughout the entire statute. However, not every word or expression used in the statute is defined in that section... occasionally the need for interpretation arises in respect of words or phrases not specifically defined in the statute, which yet bear more than one meaning in view of the text and the facts of the particular case to which the statute is to be applied."

188. The Tribunal respectfully adopts that approach. Where Parliament has not defined a statutory term, the Court must construe it according to its ordinary meaning, while remaining faithful to the context, purpose and language of the enactment.

189. The Tribunal acknowledges that general proposition. However, the ordinary meaning of a word cannot be applied in isolation from the statutory context. This was a taxing statute. The word "access" appeared in a charging provision. It therefore had to be construed with sufficient certainty to determine when tax liability arose. The Respondent submitted that "access" included the right, opportunity or ability to connect to an OTT service. The Tribunal is not persuaded that mere opportunity or technical possibility of connection was sufficient.

190. If Parliament had intended to tax availability of internet connectivity or capability to reach OTT platforms, it could have said so expressly. Instead, Parliament taxed OTT services by reference to a user's day of access, and defined OTT services by reference to the transmission or receipt of voice or messages over an internet protocol network.

191. The Tribunal reaches this conclusion for three reasons. First, the statutory definition of OTT services refers to 'the transmission or receipt of voice or messages over an internet protocol network", language that contemplates a successful access to the OTT service as contemplated by the statutory framework rather than a mere attempt. Secondly, the implementation framework adopted by UCC, the Respondent and telecommunications operators proceeded on the basis that unpaid subscribers would be prevented from obtaining access, thereby treating successful access as the relevant taxable event.

192. Thirdly, the Respondent's own methodology sought to distinguish successful from unsuccessful attempts through the application of filters and thresholds. That exercise would have been unnecessary if every attempted connection constituted access within the meaning of the Act. The statutory language therefore points to a completed or successful access event, not a mere attempt, blocked request, signalling exchange, retransmission or background data movement.

193. The Tribunal does not hold that the Respondent was required to prove the contents of a subscriber's communication. Such a requirement would neither be practical nor necessary in the context of telecommunications taxation. Equally, the Tribunal is not called upon to formulate an exhaustive definition of the term "access" under the Excise Duty (Amendment) Act, 2018. The issue is whether the Respondent established, on the evidence before the Tribunal, that the network events identified through its methodology constituted the taxable event contemplated by the Act. Once the Applicant adduced credible evidence challenging the reliability of that methodology, the Respondent bore the evidential burden of demonstrating that the identified events fell within the statutory charging provision. The determination therefore, turns on whether the assessment was founded upon a sufficiently reliable methodology capable of

distinguishing taxable access from non-taxable network activity, rather than on formulating a comprehensive definition of the word "access".

Stakeholder-Agreed Implementation Framework

194. The Applicant relied on the stakeholder implementation framework developed when OTT tax was introduced. It submitted that UCC and telecommunications operators agreed that access to OTT services would be blocked unless the customer paid OTT tax. The Applicant further submitted that it implemented this framework through the PCRF and OVA systems.

195. The Tribunal agrees that the Respondent was not bound to rely exclusively on the Applicant's internal systems or returns. The Respondent is entitled to audit and verify tax declarations independently. However, where the implementation framework was premised on blocking unpaid access through PCRF, the methodology ought to have accounted for the operation of that blocking mechanism.

196. The Respondent's methodology focused primarily on network traffic captured before the PCRF enforcement point. That was not necessarily fatal if the Respondent could demonstrate that its processing reliably excluded blocked attempts and non-taxable traffic. The difficulty is that the Respondent did not sufficiently demonstrate how, in the specific assessment, its methodology accounted for the PCRF blocking mechanism and distinguished traffic generated before blocking from traffic representing actual access.

The Applicant's PCRF Enforcement System

197. The Applicant's evidence, through AW1, AW2 and AW3, was that following the enactment of the OTT tax, telecommunications operators, the Respondent and UCC engaged on the modalities of implementation. The agreed operational approach was that users who had not paid OTT tax would be blocked from accessing OTT services. AW1 testified that the Applicant

implemented payment and access-control systems, including the Online Virtual Account and the PCRF system, to ensure that access to OTT services was granted only after payment.

198. AW2, a telecommunications engineer, explained that the Applicant's enforcement architecture involved the PCRF, PCEF and related network components. His evidence was that when a subscriber attempted to access an OTT service, the PCEF would consult the PCRF to determine whether the subscriber had paid the applicable tax. If payment had not been made, access to the OTT service would be denied. AW3 similarly testified that the PCRF operated as a gatekeeping mechanism and that non-paying subscribers could not successfully access OTT services through the Applicant's network.

199. The Tribunal acknowledges that the existence and operation of the PCRF system was central to the implementation of the OTT tax. The tax was designed to be collected by blocking unpaid access and permitting access after payment. That operational structure is consistent with the stakeholder implementation framework referred to in Exhibits A1, A2, A3, A4 and A6 respectively.

200. The Respondent did not dispute the existence of the PCRF system. Rather, it disputed whether the Applicant's internal access-control system was sufficient to disprove the independent monitoring data generated by DMS. The Tribunal agrees that the mere existence of the PCRF system does not automatically prove that no under-declaration occurred. Systems can fail, configurations can be imperfect, and independent revenue assurance may reveal matters not captured by taxpayer records.

201. However, where the Respondent's assessment depends on treating network activity as taxable access, the PCRF system becomes highly material. If traffic is captured before the PCRF has finally permitted or denied access, then such

traffic may include non-taxable attempts. The Tribunal must therefore consider whether the evidence establishes that blocked or unsuccessful attempts were sufficiently excluded from the data used to generate the assessment.

The GTP Region, the Gi Region and the Limits of Subscriber Identification

202. A central plank of the Applicant's case was that the Respondent's probe was located in the GTP Region, whereas actual internet access occurs in the Gi Region after the Applicant's policy enforcement mechanisms have operated. AW2, Mr. Michael Kizza, testified that the GTP region captures broad and unsegregated network activity, including signalling traffic, failed connection attempts, retransmissions, blocked communication and system-generated activity occurring before the Applicant's enforcement mechanisms. He explained that the Applicant's PCRF/PCEF system, referred to during the proceedings as the "Gateman", determines whether a subscriber has paid OTT tax and either permits or blocks access.

203. The Respondent's technical witness, RW1, Mr. Laurent Fiacre Sarr, testified that the DMS collected data from interfaces that preserve subscriber identifiers, including IMSIs and MSISDNs, and that the Gi interface is affected by Network Address Translation, making subscriber-level identification difficult. He explained that the DMS relied on Gn/Gp and S5/S8 interfaces because they allow traffic to be linked to identifiable subscribers.

204. The Tribunal finds that the Respondent had a legitimate technical reason for avoiding the Gi interface if NAT prevented reliable subscriber identification. The Tribunal further finds that a monitoring system may legitimately collect data at a point in the network where subscriber identifiers are preserved. However, the technical justification for capturing data at the GTP Region does not without more establish that the resulting data accurately represents successful OTT access. A system may correctly identify a subscriber yet still erroneously classify the subscriber's activity as taxable access. The evidence

establishes that traffic captured at the GTP Region may include both successful and unsuccessful attempts to OTT services. RW1 accepted during cross-examination that the GTP Region captures traffic before it reaches the Applicant's PCRF/PCEF enforcement mechanisms and that unsuccessful attempts may generate traffic records.

205. The Tribunal finds that the Respondent's evidence was stronger on subscriber attribution than on taxability. While the Respondent established that the GTP Region was technically appropriate for identifying subscribers prior to Network Address Translation, it failed to demonstrate, to the required standard of proof, that the DMS reliably distinguished successful access to OTT services from blocked or unsuccessful attempts across the assessment period. The core legal issue remains whether the identified subscriber infact accessed an OTT service so as to trigger liability under the law.

206. It is possible that some portion of the traffic identified by the Respondent represented unpaid taxable access. However, possibility is not the standard by which assessments are tested. The issue is whether the evidence establishes, with sufficient reliability, that the assessed figure represents unpaid taxable access rather than a mixture of taxable and non-taxable network events. The greater the uncertainty regarding the composition of the assessed figure, the greater the difficulty in treating the resulting assessment as accurate.

207. The Tribunal emphasises that it does not reject GTP-derived data as inherently unreliable. Indeed, the evidence establishes that GTP interfaces may provide important information concerning subscriber attribution. The difficulty arises not from the source of the data itself, but from the absence of a sufficiently demonstrated process linking that data to the statutory concept of unpaid taxable access.

208. The Tribunal therefore finds that data captured in the GTP Region could be a legitimate starting point for analysis, but it could not, without adequate filtering and validation, conclusively establish taxable OTT access.

The 1KB Threshold

209. The Applicant challenged the Respondent's use of a 1KB threshold as a determinant of access. It submitted that the threshold was not provided for under the Excise Duty Act, any subsidiary legislation, or any stakeholder agreement. It further argued that the threshold was introduced retrospectively after the OTT tax regime had been repealed.

210. The Respondent's position was that the 1KB threshold was not itself the tax law but part of the analytical methodology used to distinguish successful OTT sessions from signalling traffic and blocked attempts. RW2, Mr. Grace Aine Ngabirano, testified that the Respondent applied the threshold as part of its audit methodology and that traffic below that threshold was likely to reflect unsuccessful or incomplete attempts, while traffic above that threshold evidenced successful access. RW2 accepted, however, that the threshold was not prescribed by the Excise Duty Act, subsidiary legislation, or any formal stakeholder agreement.

211. The Tribunal agrees that the Respondent may use administrative thresholds and technical filters in an audit. When dealing with digital services, the Respondent is permitted to use technology, sampling, filters, and data analytics. The issue, however, is whether the 1KB threshold was sufficiently grounded in law and evidence to support a tax assessment of Shs. 33,911,117,000.

212. No provision of the Excise Duty Act or subsidiary legislation was produced to show that Parliament adopted 1KB as the determinant of taxable OTT access. Nor was the Tribunal shown a binding implementation instrument, agreed by

all relevant parties, establishing 1KB as the legal or technical standard for access. The Respondent described the threshold as a technical validation measure. Even if accepted as such, it remained an audit assumption capable of informing or justifying further investigation. Without further evidential validation demonstrating that the identified network events constituted the statutory taxable event, however, it could not, of itself, prove liability under the Excise Duty (Amendment) Act, 2018. This is particularly so in light of the principle applied in ***Commissioner General, URA v Kajura CA No 9 of 2015*** and as stated in ***Partington v Attorney General (1869) LR 4 HL 100***, that liability to tax must be found within the charging provision itself and not in administrative assumptions adopted for purposes of implementation.

213. The Applicant adduced evidence, through AW2's demonstration, that traffic exceeding 1KB could be generated even where a communication was blocked and no OTT message was transmitted. The Tribunal has considered that demonstration together with the accompanying technical explanation and finds that it materially weakens the assumption that traffic exceeding 1KB necessarily represents successful access.

214. The Tribunal therefore finds that the 1KB threshold was technically unsafe as a conclusive proxy for taxable access. A blocked attempt capable of generating traffic above 1KB could be counted as access if the methodology was not sufficiently refined. The Tribunal further finds that the uncertainty in the charging provision made reliance on an extra-statutory threshold particularly problematic. Where Parliament did not define access by reference to data volume, the Respondent could not convert a data-volume threshold into the practical equivalent of a charging rule. The threshold may have been useful for screening. It was not sufficient proof of tax liability.

215. The Tribunal's concern is not that the Respondent employed a threshold or that the threshold was low, high, conservative, or aggressive. Thresholds and

filters are commonly used in telecommunications analytics. The concern is that the Respondent invited the Tribunal to treat the threshold as sufficiently indicative of the statutory taxable event without demonstrating that the threshold consistently distinguished successful access from unsuccessful access throughout the assessment period. On the evidence before the Tribunal, the 1KB threshold was not shown to have a statutory basis. Nor was it sufficiently demonstrated, on its own or in combination with disclosed filtering rules, to reliably establish taxable access.

Assessment of Respondent's Electronic Demonstrations: REX 7, REX 8, REX 9 and REX 10

216. The Respondent relied on electronic demonstrations marked REX 7, REX 8, REX 9, and REX 10.

217. REX 7 was relied upon to demonstrate data capture from the Applicant's core network. The Tribunal accepts that the Respondent demonstrated that data could be captured from the relevant network environment. However, proof of data capture is not proof of taxable access. The Applicant's criticism that REX 7 showed activity in the monitored network environment before final access determination was not adequately answered. The Respondent did not demonstrate, through REX 7, how blocked attempts were separated from successful access. The Applicant also raised a concern that the timestamp in REX 7 referred to 2025, whereas the assessment period was April 2020 to June 2021. The Tribunal does not treat that discrepancy as automatically fatal to the entire assessment. However, it reduces the exhibit's probative value as evidence of what occurred during the assessment period.

218. REX 8 was relied upon to show the IPDR application, extraction, and processing of sample data. The Applicant pointed out that REX 8 reflected zero blocked OTT accesses for 1 May to 5 May 2020. Given that the PCRF blocking mechanism was central to the implementation of the tax, a result showing no

blocked accesses over that period called for a clear technical explanation. No adequate explanation was provided. The absence of blocked accesses in that demonstration supports the Applicant's concern that the Respondent's monitoring or reporting logic may not have reliably identified blocked attempts.

219. REX 9 was relied upon as part of the Respondent's demonstration of detection and processing logic. The Tribunal accepts that the Respondent presented a system capable of classifying traffic using multiple parameters, including IP addresses, certificates, proprietary protocols and bandwidth characteristics. However, the exhibit did not sufficiently demonstrate how the system excluded paid users, weekly bundles, monthly bundles, third-party payments and blocked attempts before arriving at the final assessed figure.

220. The Tribunal has carefully considered the Respondent's submission that the DMS did not rely solely on the 1KB threshold but also incorporated destination IP addresses, application certificates, proprietary protocols, traffic-flow characteristics and other technical indicators. Had the Respondent demonstrated how those indicators collectively and consistently isolated successful unpaid OTT access from signalling traffic, blocked attempts, paid access and other non-taxable network activity, that methodology may have provided a reliable evidential foundation. However, the Respondent did not disclose the filtering logic, weighting, validation process or reconciliation steps by which those indicators ultimately translated into the assessed liability. Accordingly, the Tribunal's concern is not with the use of multiple indicators as such, but with the absence of sufficient evidence demonstrating that their combined application reliably identified the statutory taxable event.

221. REX 10 was relied upon to show deduplication of accesses within a twenty-four-hour period. The Tribunal accepts that avoiding duplicate counting is an important feature of any lawful assessment under a "per user per day" charge. However, deduplication does not answer the prior question whether the

counted event was taxable in the first place. Counting a subscriber only once in twenty-four hours does not cure the error if the counted event was a blocked attempt, a paid access, VPN traffic wrongly included, or non-OTT activity.

222. The Tribunal therefore finds that REX 7 to REX 10 showed that the Respondent had a monitoring and processing system. They did not, however, provide a sufficiently complete audit trail linking raw captured data to unpaid taxable OTT access for the assessment period.

OVA Payment Records

223. The Applicant relied heavily on the Online Virtual Account as the agreed platform for recording OTT tax payments. AW1 testified that the OVA recorded OTT payments in real time and was accessible to the Respondent for revenue assurance purposes. The Respondent submitted that OVA records reflected aggregate collections and lacked the network-level granularity needed to determine actual access events.

224. The Tribunal observes that OVA records do not establish that a subscriber accessed an OTT service. Payment records and access records serve distinct evidential purposes. However, the Respondent's assessment was not confined to an allegation of access alone . It was expressly premised on access to OTT services without corresponding excise duty being declared. Payment status was therefore an essential constituent element of the liability asserted by the Respondent. The Tribunal finds that in those circumstances, OVA records were not peripheral. They were directly material to determining whether the alleged access was infact unpaid and therefore gave rise to the disputed liability.

225. The Tribunal does not hold that reconciliation with OVA records would in every case eliminate all discrepancies arising from the DMS. However, whereas here, the Respondent based its assessment on an allegation of "access without payment", and where contemporaneous payment data exists within an

agreed implementation framework between the parties, the Tribunal finds that reconciliation with such data is a necessary safeguard against overstatement and assessment on an incorrect basis.

226. The Applicant gave the example of IMSI 64110100330202015. The Applicant contends that the Respondent treated this IMSI as having accessed OTT services without payment, yet OVA records showed that OTT tax had been paid during the relevant period. The Respondent did not rebut this evidence by producing corresponding reconciliation records or explaining why the IMSI nevertheless remained classified as unpaid. Nor did it show that the entire DMS output had been reconciled against OVA payment records before the assessment was maintained.

227. The Tribunal considers this point significant because the assessment was predicated not merely upon access, but upon alleged access for which the corresponding tax had not been declared. If payment records were available in real time and accessible to the Respondent, reconciliation with OVA data was a direct way of testing whether alleged accesses were unpaid. The absence of meaningful reconciliation diminishes confidence in the accuracy of the final assessed figure.

228. The statutory function of an additional assessment is to arrive at the correct tax payable. It is not sufficient for the Respondent to rely on inferred network behaviour where available payment data may contradict the inference. The failure to reconcile DMS outputs with OVA records materially undermined the reliability of the assessment. In a case of this magnitude, involving more than 169 million alleged undeclared accesses and an assessment exceeding Shs. 33 billion, the Tribunal would ordinarily expect to see a demonstrable audit trail capable of tracing the progression from raw data capture through filtering, validation, reconciliation and computation to the final assessed figure. The Tribunal was not presented with such an audit trail.

Failure to Identify Specific Taxable Transactions

229. The Applicant submitted that the Respondent failed to identify specific taxable transactions. It argued that a lawful assessment required proof of the relevant subscriber, the relevant day, the relevant OTT service accessed, and non-payment of tax. The Respondent submitted that the DMS produced subscriber-level reports and that the Applicant was provided with sample data. RW2 testified that the Respondent engaged the Applicant in reconciliation exercises and requested corresponding data for like-for-like comparison.

230. The Tribunal accepts that in a telecommunications environment involving millions of electronic records, the Respondent is not required to tender evidence of every individual transaction relied upon in raising an assessment. Nevertheless, the Tribunal finds that any assessment must remain capable of objective verification and must demonstrate a rational connection between the aggregate liability assessed and the underlying taxable transactions alleged to be the taxable events.

231. The evidence before the Tribunal demonstrates material deficiencies in that regard. AW3, Mr. Mackinon Kabarole, testified that despite repeated requests during the audit and objection process, the Respondent did not disclose the detailed workings or identify the specific IMSIs said to have accessed OTT services without payment. During cross-examination, RW2, Ms. Grace Aine Ngabirano, further admitted that the Respondent did not reconcile the Data Monitoring System (DMS) data against the Applicant's Online Virtual Account (OVA), notwithstanding that the OVA contained the actual payment records for OTT tax.

232. The Applicant also produced Exhibit A26, in which a sample subscriber identified by IMSI 64110100330202015, whom the Respondent had treated as non-compliant, was cross-checked against the OVA records. Those records demonstrated that the subscriber had in fact paid OTT tax on 3rd, 4th and 5th

May 2021. That evidence was not satisfactorily rebutted. In the Tribunal's view, this example illustrates the absence of a sufficiently reliable reconciliation between the Respondent's technical data and the Applicant's payment records. Accordingly, the Tribunal finds that the Respondent did not sufficiently identify, either through individual transactions or through an adequately verified reconciliation methodology, the taxable transactions upon which the assessment was founded.

IP Address Classification, IMSI Anomalies and Data Integrity

233. The Applicant also challenged the integrity of the Respondent's dataset. First, the Applicant relied on correspondence from Meta Platforms Inc., referred to as Exhibit A17, indicating that some IP addresses that the Respondent treated as associated with Facebook or WhatsApp did not belong to Meta-operated services. Secondly, the Applicant relied on Exhibit A16 and related evidence to show that certain IP addresses used in the Respondent's assessment did not appear on the official list of OTT service addresses. Thirdly, AW3 testified that certain IMSIs appearing in the Respondent's data did not conform to the Applicant's standard fifteen-digit IMSI structure. Fourthly, AW3 referred to a table in his witness statement identifying 158,840 IMSIs for which the Respondent recorded network activity while the Applicant's corresponding records reflected zero bytes of usage.

234. The Respondent answered that its methodology did not rely solely on IP addresses but used multiple parameters, including application certificates, proprietary protocols, and bandwidth utilisation. It also submitted that IMSI anomalies were immaterial, accounting for only approximately 0.01 per cent of the data.

235. The Tribunal observes that not every anomaly invalidates an assessment. Large technical datasets may contain imperfections. The question is whether the imperfections are immaterial or whether they affect confidence in the

methodology. In this case, the anomalies must be considered cumulatively. The assessment depended on accurate subscriber identification, accurate OTT platform classification, accurate exclusion of non-taxable traffic, and accurate linkage to non-payment. In that context, the IP and IMSI concerns were not trivial. They reinforced the need for the Respondent to provide a complete, verifiable audit trail.

236. The Tribunal therefore finds that the data-integrity concerns, while not independently decisive, materially support the Applicant's broader case that the assessment was not shown to be reliable.

VPN Traffic Treatment

237. The Applicant also submitted that VPN-related traffic was improperly included in the Respondent's analysis, contrary to implementation discussions and the technical realities of VPN blocking. The Respondent's contention was that DMS separately identifies and segregates VPN traffic and that VPN traffic was not included in the final computation of OTT accesses.

238. The statutory definition of OTT services included access to a virtual private network. However, the evidence and submissions showed that stakeholders recognised practical challenges associated with VPN detection and blocking. The Applicant's witnesses testified that VPN applications evolve continuously and cannot be completely blocked.

239. The Tribunal considers that the mere existence of VPN traffic does not necessarily invalidate the assessment. The relevant question is whether the Respondent's final computation included VPN traffic in a manner inconsistent with the applicable law and methodology. The Respondent asserted that VPN traffic was segregated, but again did not disclose sufficient underlying filtering logic for the Tribunal to verify that assertion.

240. Further yet, the VPN treatment illustrates the broader uncertainty created by the charging provision and the implementation framework. Where the statute included VPNs within the definition of OTT services, but the assessment methodology allegedly segregated or excluded VPN traffic, the Tribunal expected a clear explanation, supported by the underlying data and computation methodology, regarding the treatment of VPN traffic and its relationship to the final assessed figure.

241. Accordingly, the VPN issue is not determinative on its own, but it forms part of the broader concern regarding the transparency and verifiability of the Respondent's methodology. The Tribunal therefore treats the VPN issue as another reason why the final assessed figure could not be accepted without a complete audit trail.

242. The Tribunal has deliberately examined the evidence relating to the PCRF records, GTP/Gi interfaces, OVA reconciliation process, IMSI data and associated system architecture because each formed an essential component of the Respondent's methodology for identifying taxable events. The purpose of that analysis was not to determine whether the Respondent's technology functioned generally or whether the GVG platform was capable of processing telecommunications data. Rather, the issue was whether the combined methodology demonstrated, to the requisite standard, that the events ultimately assessed corresponded to taxable access within the meaning of the statute. The Tribunal's conclusions therefore rest not upon isolated technical deficiencies but upon the cumulative evidential effect of the entire methodology presented.

Extrapolation from the five-day sample

243. The Applicant challenged the use of a five-day sample covering 1-5 May 2021. It is submitted that the assessment covered April 2020 to June 2021 and that the Respondent failed to demonstrate that the sample was representative of

the entire assessment period. The Respondent's evidence was that sample data was provided to facilitate reconciliation and that the assessment was based on DMS analysis. RW2 acknowledged that sample data were used and that results were extrapolated across the wider period.

244. Sampling is a useful audit tool, especially where full population testing is impractical. Tax administration would be impractical if revenue authorities were prohibited from using samples in all data-heavy audits. However, where sampling is used to support an assessment of this magnitude, the sample must be shown to be representative or otherwise statistically and methodologically reliable. The Tribunal must be satisfied that the sample is representative, that the assumptions underlying the extrapolation are disclosed, and that the resulting assessment can reasonably be regarded as reliable.

245. In this case, the Tribunal was not provided with sufficient evidence explaining the basis on which the five sample days were selected, why those days were representative of the entire assessment period, what statistical controls were applied, how exceptional events, network changes, promotions or bundle patterns were treated, how weekly and monthly OTT bundles were accounted for, how third-party payments were accounted for, how blocked attempts were excluded, how VPN traffic was treated and how the final extrapolated figure was reconciled with OVA payment records. The absence of such an explanation is material because network usage may vary by date, user behaviour, promotions, enforcement changes, VPN trends, outages, application changes and payment patterns.

246. The Tribunal therefore finds that the Respondent did not sufficiently justify extrapolation from the five-day sample to the entire assessment period.

Disclosure of Data and Methodology

247. The Applicant submitted that the Respondent failed to disclose all data upon which the assessment was based. The Respondent argued that it provided sample datasets, summaries and explanations sufficient to enable the Applicant to challenge the assessment.

248. The Tribunal recognises that URA must not, in every case, disclose every line of raw data, every algorithm, or source code used in a digital audit. Practical, confidentiality and security concerns may arise. However, where the assessment depends on a technical process known primarily to the Respondent and its service provider, the Respondent must disclose sufficient information to enable the taxpayer and the Tribunal to understand how the liability was computed.

249. During cross-examination, RW1, Mr. Laurent Fiacre Sarr, made a number of significant admissions regarding the operation of the Data Monitoring System. He acknowledged that the information displayed during the REX 7 demonstration was unstructured data, which required further processing before it became meaningful for analytical purposes. He further recognised that the system did not retain raw signalling data after processing and that technical errors could potentially be introduced during that processing. These admissions significantly reduced the evidential weight of the processed outputs because the Tribunal was unable to evaluate whether the processing methodology faithfully preserved the underlying data from which the assessment was derived.

250. RW1 also confirmed that the DMS did not cross-reference subscriber payment information contained in the Applicant's Online Virtual Account before identifying accesses for revenue assurance purposes. Finally, the evidence demonstrated that aspects of the analytical process involved manual manipulation of extracted data, including spreadsheet inputs illustrated during

the REX 10 demonstration. Although none of these matters, standing alone, necessarily invalidates the assessment, they underscore the need for a transparent and verifiable audit trail demonstrating how the processed data was transformed into the final tax assessment.

251. The Respondent disclosed processed data and sample data. But the evidence does not show that it disclosed the complete business rules, filtering logic, computations, reconciliation outputs and validation steps necessary to verify the assessment. This was especially important because the Applicant had raised specific technical objections. The Tribunal finds that the Respondent's disclosure was insufficient to sustain an assessment of this complexity and magnitude.

Whether the Applicant discharged the burden

252. The Applicant bore the legal burden of proving that the assessment was excessive or erroneous. It was not enough for the Applicant to merely to raise doubts. It had to adduce evidence showing that the assessment was not properly made.

253. The Respondent submitted that the Applicant failed to disprove the assessment and that the Applicant's internal records could not override independent revenue assurance data. We acknowledge that taxpayer records are not conclusive merely because they are taxpayer records. The Respondent is entitled to test them against independent evidence.

254. However, the Applicant did not merely rely on its filed returns. The Applicant adduced evidence through AW1, AW2 and AW3. It provided technical and documentary evidence showing material defects in the Respondent's methodology, including evidence of PCRF blocking, evidence that blocked attempts could generate measurable GTP traffic exceeding the 1KB threshold, evidence that the Respondent's monitoring point captured activity before final

access determination, evidence of OVA payment records contradicting at least some alleged non-compliance, demonstration videos, evidence of IP address classification concerns, evidence of IMSI anomalies and evidence challenging the extrapolation from a limited sample.

255. The Tribunal is satisfied that this evidence went beyond mere denial. It raised substantial doubt as to whether the assessment accurately measured taxable OTT access. Once that evidential burden was discharged, the Respondent had to provide a sufficiently clear explanation of how the assessment was derived and why the Applicant's objections did not affect the result.

256. The Respondent provided technical evidence through RW1 and audit evidence through RW2. Their evidence established that the DMS was an independent monitoring system, that it captured data from the Applicant's network, and that it used technical indicators to identify OTT traffic. However, their evidence did not sufficiently bridge the gap between captured network activity and taxable unpaid access under the Act.

257. The Tribunal therefore finds that although the Respondent had authority to audit and verify the Applicant's declarations using independent systems, it failed to establish that the impugned assessment was derived from a methodology that reliably identified taxable OTT accesses for which tax had not been paid.

258. The Tribunal emphasises that the deficiencies identified are not minor procedural imperfections or isolated technical anomalies. They relate directly to the identification of the statutory taxable event, namely whether an identifiable subscriber accessed an OTT service without payment of the prescribed excise duty. Consequently, the defects identified go to the reliability of the assessment itself rather than to peripheral aspects of the audit process.

259. We are satisfied that the Applicant has established, on a balance of probabilities, that the assessment was excessive and that the objection decision ought to have been made differently.

260. For the reasons set out above, the Tribunal makes the following findings –

(i) OTT tax was chargeable under paragraph 13(b) of the Second Schedule to the Excise Duty (Amendment) Act, 2018, on a user per day of access to OTT services. The taxable event was access to OTT services and not on-network activity generally.

(ii) The legislation did not prescribe objective technical indicators of "access".

(iii) The Respondent's use of data captured from the GTP Region was not unlawful per se. However, because that region captures both successful and unsuccessful attempts before enforcement controls are applied, the Respondent was required to demonstrate adequate filtering and validation. It did not do that to the required standard.

(iv) The 1KB threshold had no statutory basis and was not shown to be a sufficiently reliable proxy for taxable access, particularly in light of the Applicant's evidence that data exceeding that threshold could be generated without successful OTT communication.

(v) The treatment of blocked attempts was not sufficiently demonstrated.

(vi) Reconciliation between DMS outputs and available OVA payment records was not shown, despite evidence that the OVA recorded payments in real time and was accessible to the Respondent.

(vii) The cumulative effect of the unresolved IP address concerns, IMSI anomalies and VPN-related issues materially undermined the reliability of the assessment methodology and, consequently, the accuracy of the assessment.

261. The Tribunal has not approached the evidence on the basis that the Applicant's experts were necessarily correct and the Respondent's experts necessarily

mistaken. Rather, the Tribunal has evaluated the competing expert evidence against the statutory framework, the contemporaneous implementation arrangements, the documentary exhibits, the electronic demonstrations, and the internal consistency of the competing explanations. Where the Tribunal has preferred aspects of the Applicant's evidence, it has done so because those aspects were corroborated by contemporaneous documents, demonstrated through practical testing, or were not satisfactorily answered by the Respondent's evidence.

262. In preferring significant aspects of the Applicant's technical evidence, the Tribunal has not done so merely because the Applicant called more witnesses or because those witnesses possessed specialist expertise. Rather, AW2's evidence regarding the operation of the PCRF/PCEF architecture was consistent with the contemporaneous implementation documents, the stakeholder records and the practical demonstrations conducted before the Tribunal. AW3's evidence concerning reconciliation, sampling and data integrity was supported by documentary exhibits, including the correspondence exchanged during the audit and objection process. By contrast, important aspects of the Respondent's methodology remained insufficiently explained notwithstanding the evidence of RW1 and RW2. RW1 accepted that the system did not retain raw signalling data after processing and acknowledged the possibility of processing errors, while RW2 accepted that the DMS analysis did not utilise the Applicant's OVA payment records and that the 1KB threshold formed part of the Respondent's analytical methodology rather than the statutory framework. Those admissions materially informed the Tribunal's evaluation of the competing expert evidence.

263. We note that large-scale telecommunications monitoring systems inevitably involve assumptions, approximations and technical limitations. We would thus not set aside an assessment merely because an individual anomaly, discrepancy, or methodological weakness had been identified. However, the

present case must be assessed cumulatively. The uncertainty surrounding the statutory concept of access, the reliance on a non-statutory threshold, the evidence regarding blocked traffic, the absence of demonstrated reconciliation with payment records, the questions raised regarding IP classification and IMSI integrity, the treatment of VPN traffic, and the limitations of the sampling exercise must be viewed together.

264. When viewed cumulatively, those matters substantially diminish confidence that the assessed figure of 169,555,586 alleged undeclared accesses accurately represented unpaid taxable OTT access. It is the combined effect of these concerns, rather than any single concern in isolation, that ultimately leads the Tribunal to conclude that the Applicant has discharged the burden imposed by section 19 of the Tax Appeals Tribunal Act.

265. Accordingly, issue one is resolved in favour of the Applicant.

Remedies

266. Section 20 of the Tax Appeals Tribunal Act empowers the Tribunal to affirm, vary, set aside, substitute or remit a taxation decision. Having found that the assessment was excessive and erroneous, the Tribunal sets aside the additional assessment of Shs. 33,911,117,000, and the objection decision confirming the same.

267. The Tribunal is satisfied that this is not an appropriate case for remittal. Remittal may be appropriate where a correct assessment can be achieved by correcting a discrete computational error or curing a limited procedural defect. That is not the position here. The deficiencies identified by the Tribunal are foundational rather than incidental. They concern the identification of the statutory taxable event, the evidential sufficiency of the Respondent's methodology, including the use of the 1KB threshold, the treatment of blocked attempts, the failure to reconcile alleged OTT access with the Applicant's

payment records, and the absence of a demonstrable link between the network activity captured by the Respondent and the final assessed liability.

268. These are not matters capable of correction through further computation while preserving the integrity of the original assessment. The defects identified do not relate to the computation of tax from accepted primary facts. They concern the identification of the primary facts themselves. Until those foundational facts are reliably established, there exists no lawful basis upon which a fresh computation could proceed.

269. Having found that the Respondent did not establish that its methodology reliably identified the taxable event contemplated by the Excise Duty (Amendment) Act, 2018, the Tribunal is not satisfied that remittal would serve any useful purpose or result in the correction of a discrete and identifiable error. The proper remedy is therefore to set aside the objection decision and the additional assessment in their entirety.

270. The Applicant also seeks a refund of the statutory deposit paid pursuant to section 15 of the Tax Appeals Tribunal Act. Since the assessment has been set aside, the legal basis for retaining the deposit falls away. The Respondent shall refund the statutory deposit in accordance with the applicable law.

271. On costs, section 22 of the Tax Appeals Tribunal Act empowers the Tribunal to make appropriate orders. Section 27 of the Civil Procedure Act provides that costs follow the event unless the court or tribunal, for good reason, orders otherwise. The Applicant relied on **Candiru v Amandua & 2 Ors (Civil Suit 19 of 2014) [2017] UGHCCD 139 (27 October 2017)**, **Hajji Musa Hasahya v Owori & Co. Advocates (HCCA No. 71 of 2011)**, **U.T.C. v Outa [1985] (UHCB 27)**, and **Premchand Raichand Ltd v Quarry Services of East Africa Ltd and Others (No. 3) [1972] EALR 162.**

272. The general principle is that a successful party should not be deprived of costs unless there is a good reason. The Respondent was exercising a statutory audit function, and the dispute involved complex technical and legal questions. However, the Applicant was compelled to challenge an assessment that has been found to lack a sufficient legal and evidential foundation. In the circumstances, costs are awarded to the Applicant.

Orders

273. The Tribunal makes the following orders:

(i) The application is allowed.

(ii) The additional Local Excise Duty assessment of Shs. 33,911,117,000 for the period April 2020 to June 2021 is set aside.

(iii) The objection decision confirming the said assessment is vacated.

(iv) The Respondent shall refund the statutory deposit paid by the Applicant in accordance with the applicable law.

(v) Costs are awarded to the Applicant.

It is so ordered.

Dated at Kampala this **30th** day of **June** 2026.

HON. STELLA NYAPENDI CHOMBO
CHAIRPERSON

HON. PROSCOVIA REBECCA NAMBI
MEMBER

THE REPUBLIC OF UGANDA

IN THE TAX APPEALS TRIBUNAL AT KAMPALA

TAT APPLICATION NO. 134 OF 2023

MTN UGANDA LIMITED.....APPLICANT

VERSUS

UGANDA REVENUE AUTHORITY.....RESPONDENT

BEFORE: HON. STELLA NYAPENDI CHOMBO, HON. PROSCOVIA REBECCA NAMBI, MS. CHRISTINE KATWE

DISSENTING RULING

1. I have had the opportunity of reading the draft ruling of my colleagues and wish to dissent as follows;

2. In the Financial year July 2017 to June 2018, the Government amended the Excise Duty Act and included the "Over -The -Top Tax" (OTT), which came into force on 1 July 2018. Section 1 of the Excise Duty Act interprets Over-the-Top services to mean the transmission or receipt of voice or messages over the internet protocol network and includes access to virtual private networks.

3. The telecommunication companies, being the ones to administer, charge and collect the taxes, held meetings with the concerned Government bodies and discussed issues relating to the interpretation of the applicable law, implementation, applicability of the tax, the challenges faced, including the Respondent's amending of the Excise Duty returns for proper administration and compliance.

4. The Government of Uganda had contracted the Global Voice Group (GVG), a third party, to develop the Telecom Information Management System (TIMS) as a multi-tenet platform used by different entities of Government for various needs under the State House Revenue Intelligence Unit, which system picks data from the telecommunication companies directly. This GVG team developed a business intelligence platform called the Data Management System (DMS) for the UCC, the Respondent (when later included), the Bank of Uganda, and the Police Force. The Police were nominated by the Government to be the implementing agency of this system.

Mr. Laurent Fiacre Sarr's evidence

5. Mr. Laurent Fiacre Sarr, a Senegalese and a Telecommunication Engineer who has worked in several countries with Governments in matters of Telecommunications audit, including the Packet Core Monitoring Solutions for Governments in Africa, was working as a Senior Consultant in Telecommunications Big Data Processing supporting the TIMs and DMS project team under the Government of Uganda. In his Witness statement, he stated that;

6. With his experience in telecommunications, he is well-versed in mobile data and OTT-related monitoring solutions for purposes of compliance monitoring. That prior to the implementation of the DMS Platform, the Respondent was solely relying on the declarations provided by the Mobile Network Operators (MNOs) without having any means to verify the accuracy of these declarations.

7. To improve the verification processes, the Respondent introduced the DMS Platform, enabling it to cross-check MON's tax declarations. Similar to the MNO's internal processes used for reporting, quality of service monitoring, and marketing purposes, the DMS Platform collects raw data from the MNO's networks. This data is processed to facilitate a comparison with the MNO's declaration, ensuring accurate verification.

8. Mr. Laurent Fiacre Sarr gave the following points to describe the high-level description of the interfaces and logic that DMS Platform relied on in the data collection from the Applicant's network for OTT Compliance purposes:

i. **Gi interface vs Gn & S5/S8 interfaces;**

9. He stated that the Gi is the interface between the MNO's network and the Public Data Network (internet). It doesn't offer the necessary granularity to easily identify the traffic from each of the user to determine access to OTT services. The only information related to the session and many mobile networks apply Network Address Translation (NAT) on the Gi interface, where private IP addresses assigned to mobile devices are translated to public IP addresses. These further abstracts direct subscriber identification at the Gi interface level.

10. He stated that the Gn S5/S8 interfaces instead offer the possibility to identify subscribers and their respective data usage. Both interfaces connect the different core network nodes managing the Data connection of the end-user, thus making it possible to identify the data usage of each other. In the Gn & S5/S8 interfaces, the core network nodes communicate through the GTP protocol, GTPv1 and GTPV2.

ii. **Identifying the OTT Users:**

11. He testified that in a telecommunications network, the Gi interface is a reference point in the architecture, particularly for mobile networks like 3G, 4G, and 5G. It connects the Packet Gateway (PGW) or Gateway GPRS Support Node (GGSN) in the core network to external packet data networks (PDNs), such as the internet.

12. He added that identifying a subscriber (OTT user) directly from the Gi interface is not ideal because the Gi interface is designed to handle IP traffic routing between the mobile core network and external networks rather than to directly identify or manage subscriber -specific information.

13. He stated that on the Gn interface, certain identifiers and data fields are used that can be correlated back to a specific subscriber. The key elements are;

i. **IMIS (International Mobile Subscriber Identity)**

14. The IMIS is a unique identifier assigned to each mobile subscriber. It is carried within signaling messages in GTP-C (control plane) communications. When a mobile control messages, allowing the network to uniquely identify the subscriber.

ii. **MISISDN (Mobile Station International Subscriber Directory Number).**

15. Which is the mobile phone number associated with the subscriber? It might also be used in control signaling, although IMISI is more commonly relied upon for identifying the subscriber in the core network.

iii. **PDP Context (Packet Data Protocol Context):**

16. This is a data structure maintained by the SGSN and GGSN that contains information about the session, such as IP address, QoS parameters, and the subscriber's IMSI. When a mobile device establishes a data session, context is created and managed over the Gn interface. This context includes the IMSI, which directly identifies the subscriber.

iv. **IP Address Assignment:**

17. When a data session is established, the subscriber is assigned an IP address by the GGSN. The mapping between the IMSI and the assigned IP address is maintained in the PDP context, which is communicated over the Gn interface.

18. The data collection from the Gn interface was agreed on between the different technical teams from the Respondent and the MNOs before the implementation of the Platform. Several technical meetings were held between

the different parties to agree on the monitoring processes before the implementation of the Respondent Platform.

19. In addition, technical surveys were conducted by the Respondent team to further understand the MNO's network architecture and the specific nodes from which required interfaces can be mirrored. A high-level design was then shared and agreed on with the MNOs' technical team, and they then proceeded to mirror the interfaces requested. No objection from the MNOs was recorded at that specific time.

20. The purpose of the Applicant's platform, which manages OTT access, is entirely different from that of the Respondent's DMS Platform. These two platforms cannot be compared as the Applicant's platform is legally required to identify all OTT accesses and block access for the subscribers who do not pay the OTT tax.

21. In contrast, the Respondent platform is a compliance monitoring system without the capability to block OTT access. It only identifies OTT sessions from various subscribers and reports their unique accesses.

22. Consequently, it is evident that the data collection and management mechanisms for the two platforms cannot be the same. Regarding the incorrect IMSIS reported by the Applicant, it is important to note that the Respondent's platform does not generate IMSIs, but instead it simply reports the IMSIs as they are collected directly from the operator's network.

23. However, when the Respondent engaged the DMS, it raised an additional administrative assessment for Shs. 33.911.117,000 being Excise Duty on Over- The – Top Tax (OTT) for the period from April 2020 to June 2021 allegedly on the Applicant's customers accessing OTT services without paying

the Shs. 200 OTT Tax, which the applicant objected to and the Respondent upheld the Assessment, thus, this application.

24. It is therefore from the above analysis that the Respondent maintained the assessment raised against the Applicant and accordingly disallowed all the objections.

The Applicant raised several issues as follows:

25. Whether *the Respondent's assessment against the Applicant meets the legal standard in accordance with paragraph 13(b) of the Second Schedule of the Excise Duty Act 2018 as amended*

26. That the assessment was founded on assumptions, undisclosed methodologies, unverified thresholds, and data whose reliability remained disputed. He accordingly urged the Tribunal to set aside the assessment.

27. That the assessment has been disputed on both legal and technical grounds, that the assessment was founded on a methodology unsupported by statute, based on data captured at an inappropriate point in the network, and incapable of proving actual taxable access by identifiable users who had not paid OTT tax.

However,

28. The Respondent, on the other hand, maintained that the assessment was based on independent data captured from the Applicant's network, processed through the Data Management System, and subjected to audit and reconciliation processes. The Respondent argued that the Applicant had failed to demonstrate that the assessment was excessive or erroneous.

29. The Respondent reiterated that the assessment was based on information obtained directly from the Applicant's network, analysed using the DMS

methodology and subjected to audit and reconciliation procedures before the assessment was issued.

30. The Excise Duty (Amendment) Act 2018 under Section 3, amended Section 4 of the principal Act by inserting subsection (5), which provided that a telecommunications service operator providing data used for accessing over-the-top services is liable for and pays excise duty on the access to the over - the -top services and the duty payable was Shs. 200 per user per day of access under item 13(b) of the Second Schedule.
31. The Respondent defined the word access, which was not directly defined by the law, to mean the ability, permission, and technical means to avail to a subscriber to connect to, use, send, and receive internet data packets from specific-based applications, content, etc.

32. The Respondent's audit team explained that they were alive to the declarations in the return and that these were subscriptions. The data had been converted into unique access days and compared with the Applicant's data. It was also determined that the length of a day is to be 24 hours, starting from the first successful access to OTT services, which ensured that a customer would only be determined to have accessed OTT services in a day from the time they first accessed them, and the count would restart after 24 hours had elapsed. The audit team used a time–based access formula with the length of a day being 24 hours.

33. The Applicant submitted that the Respondent conflates subscriber identification with actual access to OTT services. That whereas the Gn, S%/S8 and GTP regions may contain subscriber–related traffic information, the evidence before the Tribunal demonstrates that such regions capture unsegregated traffic, including failed attempts, incomplete sessions, blocked requests and other non-chargeable traffic. The Applicant states that the mere ability to identify a subscriber within the GTP region does not establish that the

subscriber successfully accessed an OTT service within the meaning of the LED Act 2018.

34. The Applicant states that the Gi region, on the other hand, represents the point at which traffic exits the Applicant's network towards external OTT platforms through the Public Data Network (internet). That at this stage the PCRF would already have applied the Applicant's rules, including blocking customers who had not paid OTT tax and permitting compliant customers to proceed. So, the Applicant states that the Gi region reflects segregated traffic comprising customers who had successfully satisfied the conditions for OTT access.

35. Mr. Kizza (AW2) explained the distinction between the Gi and GTP regions that;

36. By use of the Applicant's mast (base Station). A customer would connect to the Applicant's network (not the internet). At this point, the customer would be in the GTP region on the Applicant's network. Then the Policy and Charging Rules Function (PCRF) would cross-check whether a customer has paid OTT tax. The payment would reflect in the Online Virtual Account (OVA) at the time of payment.

37. Upon confirmation of payment, the customer would be granted access to OTT services on the internet. Thus, the PCRF would permit the customer's transmission to the GI region (the internet protocol network). That if a customer, upon connecting to the network, without paying OTT, attempted to connect to OTT services (on the internet), the PCRF (probe) would block him or her and deny him or her access to the OTT services.

38. The Applicant maintained that it had never agreed to the Respondent relying on probes positioned within the GTP region as the basis for determining access to OTT services. That the Applicant's consistent position has been that the Respondent ought to have confirmed actual access from the Gi region,

which reflects successful and completed access to OTT platforms, rather than from the GTP region, which merely captures unsegregated traffic including failed attempts, blocked sessions, and non-chargeable traffic.

39. However, from (1) above, Mr. Sarr informed the Tribunal that "the data collection from the Gn interface was agreed on between the different technical teams from the Respondent and the MNOs before the implementation of the Platform. Several technical meetings were held between the different parties to agree on the monitoring processes before the implementation of the Respondent Platform.

40. In addition, technical surveys were conducted by the Respondent team to further understand the MNO's network architecture and the specific nodes from which required interfaces can be mirrored. A high-level design was then shared and agreed on with the MNOs' technical team, and they then proceeded to mirror the interfaces requested. No objection from the MNOs was recorded at that specific time." And Mr. Saar intimated that the Gi region does not allow identification of the IMSIS of the user.

41. I drew my attention to Exhibit REX11 tendered in by the Respondent:
It is an email trail, as follows:
From Immurana Hamza ihamza@globalvoicegroup.com dated Friday 20/09/2024 to the Respondent team and the GVG team.
It reads, "*Please find below the trailing email requesting MTN to clarify some. MSISDN (Phone Numbers) accessing OTT without paying Tax." Thank you, Hamza.*

From Kwabena Oben-Nyako kobennyarko@globalvoicegroup.com
Monday, 3 July 2023 at 09:33 To: Immurana Hamza ihamza@globalvoicegroup.com, Laurent Saar and others of GVG 'FYI"

From: Kenneth Tweheyo ktweheyo@ucc.co.ug

Subject: FW: Request for Clarity on some MSISDNs accessing OTT services without OTT Tax Payment in the MTN Uganda Network.

Hello Ronald

The team from DRI is seeing MTN numbers accessing OTT platforms without paying the OTT tax. Please help. Regards, Kenneth Tweheyo HEAD-COMPETITION AFFAIRS UCC

Another email sent on 03/03 2021 at 12:52

Dear Kenneth.

Hope this email finds you well.

Kindly be notified that we've been checking the Service Data Flows (SDFs) about the OTT users we have in the DMS platform with the OTT subscriptions found in the PCRF Files received from MTN.

We came to realize that some users (MSISDNs) have access to OTT services (e.g., Facebook) without being blocked (their flows have an important number of packets and bytes up/down) and found to have not paid the OTT tax.

Below is the list of the sample numbers; it is just a sample of MTN network subscribers from the analysis conducted on 06th January 2021. – And eight (8) numbers were listed….

42. Just above, the Consultant, Mr. Sarr, stated that they took time to observe the Applicant's system and that technical surveys were conducted by the Respondent team to further understand the MNO's network architecture and the specific nodes where required interfaces can be mirrored from. A high-level design was then shared and agreed on with the MNOs' technical team, and they then proceeded to mirror the interfaces requested. No objection from the MNOs was recorded at that specific time.

43. Mr. Laurent Fiacre Sarr is a Telecommunication Engineer and has worked in several countries with Governments in matters of Telecommunications audit. He took time to observe and decided on where to probe from. They had prior

knowledge of OTT access without payment and knew where to be; otherwise, auditors are not always told what to do.

44. They observe and choose on their own what to do and from where otherwise if they follow the direction of the owners the maybe led to already synchronized work whose results would match the return filed. So, a good auditor always devises a way of getting information that has not been laid down for him or her. The above must have prompted the audit, and they knew exactly where and what to do.

The filtering of accesses

45. The Respondent stated that the unsegregated data in the GTP region was processed to filter out unsuccessful and blocked attempts, thus separating data to align like poles and unlike poles all in their similar column.

46. The Respondent demonstrated how filtering took place, but the Applicant stated that the Respondent did not prove any efficient or verifiable filtration process that was undertaken to accurately determine access to OTT services.

47. The ***Cambridge Advanced Learner's Dictionary 4th Edition, page 572,*** defines filtration as the act of passing a liquid or gas through a piece of equipment in order to remove solid pieces or other substances. In the ***Google dictionary***, filtering means the process of removing unwanted elements, impurities, or irrelevant data from a mixture, stream, or dataset.

48. It goes on to say that filtering allows only the desired substance, signal, or information to pass through or remain, and is widely used across physical sciences, technology and daily life. This is what I observed in the demonstration carried out by Mr. Sarr. With technology, auditors use this process by way of a computer, and work moves on fast. I wonder what the Applicant wanted to see here.

49. All was demonstrated, but those who understood the process got it. Those who don't usually use it or don't have data to separate for information and audits for proper reporting still complain, but Mr. Sarr did that twice. The Respondent didn't have to cross-reference DMS data with the Applicant's Online Virtual Account.

50. All that the Respondent had to do was to compare what he has filtered as accesses, separate it in accordance with the law; i.e, a month, match it with the return, and multiply the number of accesses by 200 and get results. The Applicant has to know and remain focused on the Respondent's goal but not to go through the process that the Applicant wanted. This is because it was not beneficial to the Respondent and was a waste of time.

Elimination of multiple data.

51. The Applicant stated that the Respondent failed to eliminate multiple accesses by a single user to reflect only one taxable access per user per day; elimination of customers who had already paid OTT before accessing OTT services; elimination of customers who had paid weekly, monthly or yearly OTT bundles but accessed OTT services multiple times during the validity period of such payments.

52. In cross-examination, Mr. Grace Aine (RW2) stated that, in deriving accesses made by the Applicant's customers, the Respondent considered total daily, total weekly x7; total monthly x30; total quarterly x 90; semi-annual x 180; annual x3651/4 to arrive at accesses.

53. On being asked why he used the formula, he answered that the Applicant configured bundles that would be accessible to the customers to use the OTT applications, where a customer subscribes to a weekly bundle, and it was successfully provided or granted, they were permitted to use the OTT applications for 7 days. That daily the customers were permitted for a day.

54. For monthly, they were permitted for 30 days, and quarterly, semi–annual, and annual 90,180,365 respectfully. This had been duly demonstrated in a live demonstration at the Tribunal. He explained that in this logic, the Respondent looked at each user uniquely or distinctly, observing them on each day they made an access.

55. Counsel Agaba asked RW2 to tell the Tribunal what logic he was referring to and he replied that, it is a formula causing conditions as seen on A22 page 208 of the JTB applied on the data obtained from the GTP that users of data and what they used to access, how much and time and date it was accessed and the means i.e normal or via VPN. That the formula runs on that.

56. Mr. Agaba Richard: How did it identify the user, and how did it isolate all the multiple accesses of that user to only consider one access?

57. He responded that to begin with, he checked on the Google Dictionary and found that multiple access refers to techniques that allow multiple users or devices to share a single communication channel or frequency band simultaneously without interfering with one another.

58. In response to the question, RW2 replied that a random sample was used to demonstrate to the Tribunal how the Respondent accounted for multiple accesses in a single day for those that crossed over in the 24 hours to other days.

    However, this random IMSIS was observed to have accessed on three days, as demonstrated, and true that the same IMSIS customer had actually been accounted for by the Applicant. Therefore, it didn't form part of the assessment for three days, and this is proof that the analysis and methodology were not part of the Applicant's declarations.

59. Mr. Agaba asked Mr. Aine how the Respondent filtered out all the multiple accesses and considered one access on the 1st day of April 2020. Mr. Aine stated that 'for a customer who wakes up at 5 am on 1 April 2020 and makes

his first OTT access, the logic observed it on 1 April 2020 at 5 am provided they made a successful access. By successful, he can be seen sending and receiving messages.

60. Where this actively happens multiple times all the sessions between 5 am on 1 April 2020 till 2 April 2020 at 4:59 am are all recognized by the logic. However, the customer is only recognized as a distinct access on 1 April 2020. The Respondent looks at calendar days, but on other days, the customer is the identifier.

61. On filtering out multiple accesses to consider only one access, Mr. Aine answered that the logic observes them at 9.30am today and they are treated as accesses of OTT at 9.30 am 0n 16 December 2025. Whether they made additional accesses i.e. they continue to use OTT till tomorrow, 17 December 2025, at 9.00 am. The logic recognizes all those accesses, but still recognizes them only on 16 December 2025 once in the computation. The user or customer is given their own distinct observation from the others throughout the analysis.

62. On cross-referencing, Mr. Agaba questioned about cross-referencing for payment. Mr. Aine replied that on page 209, under the column declared, is the confirmation of payment received from the accesses as declared by the Applicant in the column declared, which, when multiplied by 200, is equivalent to the collection made by the Applicant.

63. When asked why RW2 converted the lump-sum subscriptions into weekly, monthly, annually, he replied that the law required OTT accountability to be per day of access, and though the Applicant allowed the user to pay for more than one day, which was not a problem. That the monthly was also required for filing/ declaration purposes, in accordance with the law.

64. On the use of OVA payment, the Respondent stated the team was interested in access, not payment. Once they got the access figure, they multiplied it by 200 and matched it with the declarations in the returns filed.

65. On filtering, the Applicant should learn that auditors would ask questions and know where the one being audited wants to take them and they would devise a way of going around it.

66. And on the other hand, Mr. Sarr stated that they agreed to use the GTP region at the beginning, but the Applicant just changed their mind after seeing the results. The Applicant is complaining about the unsegregated data in the GTP region and wants to take the Respondent to the GI region, where data was already synchronized.

67. The Respondent was interested in raw data and had means of filtering it to get what it wanted. Technology is now used to do work like filtering so that one gets what one wants according to the command. Of course, the Respondent did the filtering in a demonstration which many, especially non-auditors, wouldn't pick at hand.

The 5-day sample:

68. Auditors use samples to demonstrate, test, or compare among others. RW2 stated that the data was voluminous, and the Respondent team provided the 5-day sample to act as an example. The Applicant would have matched that sample with the corresponding period to maneuver it to see if it best suited all their grievances in order to sit down with the Respondent and discuss what may not have been right or why the Respondent did what it did. They just sat on it and kept on complaining without using the sample provided.

On usage of 1KB

69. The Applicant submitted that the Excise Duty (Amendment) Act 2018 did not prescribe, authorize, or contemplate the use of any threshold whether 1KB, 1MB or otherwise.

70. The ***Cambridge Advanced Learner's Dictionary on page 1634*** defines ***threshold*** as the level or point at which you start to experience something or at which something starts to happen. The Google dictionary defines ***threshold*** as a point or level where something begins, changes, or takes effect. That it broadly refers to a limit, a starting point or the physical entrance to a space. The Respondent submitted that it introduced a threshold of 1KB to aid it in determining the Applicant's customers' access to OTT services.

71. The role of the Respondent was to verify that the returns filed were accurate, which mandated the need to use the threshold to validate the said returns. The Applicant submitted that the Act did not prescribe, authorize, or contemplate the use of any threshold, whether 1KB,1MB or otherwise as a criterion for determining access to an OTT service.

72. In re-examination, Mr. Aine confirmed that the LED Act did not provide for a threshold. The Respondent needed to determine the use of the available information obtained from the Applicant, which included users of OTT services and the amount of data consumed through the downloading and uploading of information.

73. It was established that the minimum usage for both sending and receiving data was 1KB. In the same instances, the users were able to access with less than one (1) KB in a single session, as demonstrated. In the earlier submissions, therefore, the Respondent proceeded to determine access. So, the Respondent determined access for every customer that exceeded 1KB in a

single session. In all considerations, the threshold was helping the Respondent in having the declared accesses.

74. What I take from this is that, the Respondent applied a threshold on its own as a tool to pick accesses for data purposes. However, this sort of helped the Applicant to minimize the assessment by a small figure. The Respondent was supposed to take all access, however small. The law implied all accesses not to segregate that this is very small; then we leave it out and start with this, however small the number left untaken. This did not necessitate inclusion in the law as it was just applied in picking data.

75. The Applicant shared an online virtual account, the OVA with the Respondent at the time of the implementation of OTT and on inquiring whether the Respondent used it, Mr. Aine responded that the Ova is an online virtual account which is a record of collections/payment. And Mr. Agaba wanted to know whether the Respondent ever used it. Mr Aine responded that the Respondent required only access to multiply with 200 and cross reference with the payments made. The auditor will always fall on his final findings instead of cross-referencing what has been arranged before.

On truncated IMSIs

76. The Google dictionary defines the words truncated iMISs to mean an incomplete international mobile subscriber identity.

77. The Applicant stated that the information shared by the Respondent contained IMSISs that did not conform to the Applicant's nomenclature, which is 15 numeric digits. Meaning that they were unknown to the Applicant. RW2 replied that the Respondent put its plug on the Applicant's system and picked up information from there. These numbers are not able to transact if they are not proven by UCC.

78. Mr. Aine replied that they were 0001 and so immaterial to the audit. While the Applicant submitted that they undermined the credibility of the Respondent's audit, RW2 stated that they were found on the Applicant's system and picked from there.

79. On the treatment of VPNs, the Applicant stated that while it was agreed that VPNs should be left out of the audit, the Respondent's own workings, processed data, and underlying records still contain references to VPN. On the filtering demonstration done by RW1, VPNs were indicated at filtering and they were set aside with other unwanted data.

In conclusion

80. Before the OTT, the Government contracted and engaged GVG to manage and control Cinematography, Money Laundering etc. That is why GVG was here before and was under the control of Statehouse but the institutions in charge were the Uganda Communication Commission (UCC) Uganda Police and Bank of Uganda. When the Government introduced OTT, it included the Respondent (URA) on the list.

81. Of course, the Law was put in place and the institutions involved i.e. UCC, URA and the Mobile Network Operators (MNOs) that is, MTN, Airtel and others sat together and discussed the modalities, infrastructure and architecture of how this tax will be administered for appropriate execution to completion. Several meetings were held and all the parties agreed on the modalities. The MNOs i.e. Applicant took the GVG through its infrastructure and they agreed on where to place the GVG home within the Applicant's structure to start their work.

82. It is clear how the UCC staff could see what was happening to the extent of exchanging emails between themselves on OTT access granted to non-payers of the Shs. 200. The UCC observed this and was communicating to

themselves and the GVG. Definitely, after going through the infrastructure and architecture, the GVG knew where to be placed with their experience.

83. First of all, there was nothing wrong with the Law, it was clear. The name of the tax, where to be placed, the duration i.e 24 hours, to be charged on access, how to be declared, what period of accountability i.e; 1 month, and as LED in the LED return, which was amended to include the OTT section. Definitely, the Law could not go into the nitty-gritties. If every section went into the nitty-gritty of the law, then the book would be so voluminous. The URA, as usual, was the administrator of the tax and is always welcome to any queries and clear explanations, name it. There were no complaints, and no Regulation was made as everything was clear.

84. Regarding the audit done, the parties involved sat together and agreed on how to handle the issues involved, and the telecom companies were not new to LED, as it had been running in their sector for a long time. On issuing the assessments, the Applicant objected as usual, crying foul that the law did not mention this and that

85. The GVG has its reputation and experience, and the person heading it is a telecom engineer with enough experience around Africa. This twist of "No law mentions this" are all techniques used to deter tax collection. It is rare to find an auditor who succumbs to the orders of the auditor is auditing that come and audit me from this area.

86. It shows that he is driving you to where he knows he will feel comfortable, as the auditor would not uncover any wrongdoing but find well-packaged information to match the declaration. The problem would not be solved. The issue is not catching and penalizing, but whether what was done matches the law.

87. The question is, did everyone who accessed the internet at the time pay the OTT as the law prescribed? Pay 200 for 24 hours. If it is a group like a conference in one room with one access, how do you then treat it? Is it a multiple access? What does the law say about every access?

88. All this, the Respondent has answered and supported its assessment. They have gone ahead and explained multiple access, the 24-hour scenario which doesn't match the 24-hour calendar time, the filtering exercise of how they separated several types of scenarios like WhatsApp, Facebook, use of VPNs, etc, the threshold used and why, the truncated IMSI, the GI and the GTP, but to no heed.

89. To me, the government did its work. It imposed the Law, enacted it and enforced it, and where compliance was not appropriate, it came up with the results of Shs. 33,911,117,000 to fill the gap that was created between the practice and compliance.

90. In light of the above, I find that:
    i. The objection decision stands.
    ii. The Applicant pays the Shs. 33,911,117,000.
    iii. This Application is dismissed with costs to the Respondent.

Dated at Kampala this **30th** day of **June** 2026.

MS. CHRISTINE KATWE

MEMBER