xintec

CASE STUDY IN REVENUE ASSURANCE

Capturing Roaming Data and Billing for It

Introduction

Many telecom operators don't believe that Revenue Assurance is a valuable function.

If a vendor attempts to sell a revenue assurance system, very often the network operator's natural assumption is that carrying out checks on data is a futile exercise, because errors are highly unlikely in their environment.

But this is far from the truth.

And because the network operator doesn't believe there are errors, they might say “OK fine, audit our data, and see if you can find some errors”.

In Revenue Assurance, we perform many reconciliations to ensure accuracy and completeness of billing and data capture.

One essential area is billing for inbound roamers—subscribers from other (roaming partner) networks using services on your home network.

Despite its seeming simplicity, errors can and do occur, leading to significant financial implications and operational embarrassments.

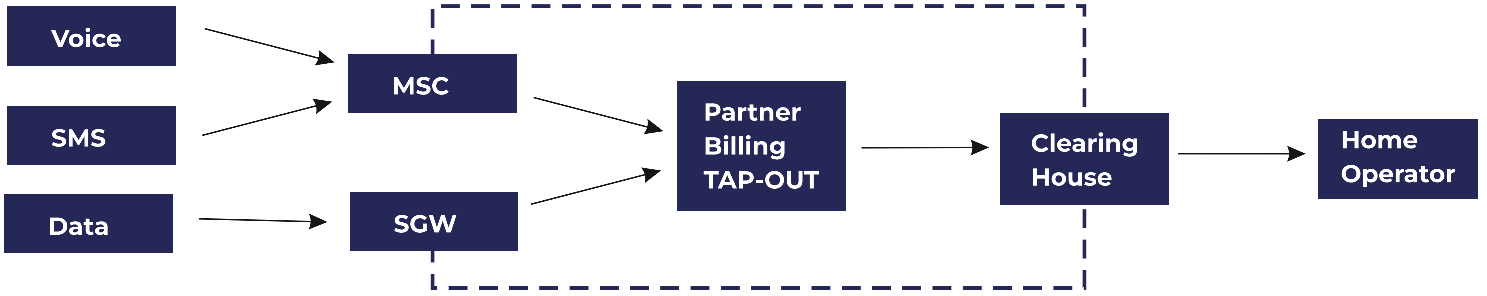
The Problem

Recently we identified an issue in an archipelago, where each of the small islands are host to multiple competing network operators.

In this case, one of the islands' operators noticed that a high percentage (45%) of mobile originated (MOC) voice calls generated by inbound roamers were missing from TAP-OUT files.

This resulted in significant revenue loss for the subscriber's home network operator due to unbilled usage.

The process flow:



Subscribers use services on the visited network (voice, SMS, data) when roaming

Usage data is captured by the visited network switches: MSC for voice, SMSC for SMS, SGW for data

Event data records are sent to the billing system. Each record is tagged with charges based on usage (e.g. call duration, number of SMS) Records are compiled into TAP-OUT files

TAP-OUT files are (most commonly) sent to a clearing house for billing the home operator

TAP-OUT (and other information) is forwarded to the home operator

Key Learnings Continues

The Solution

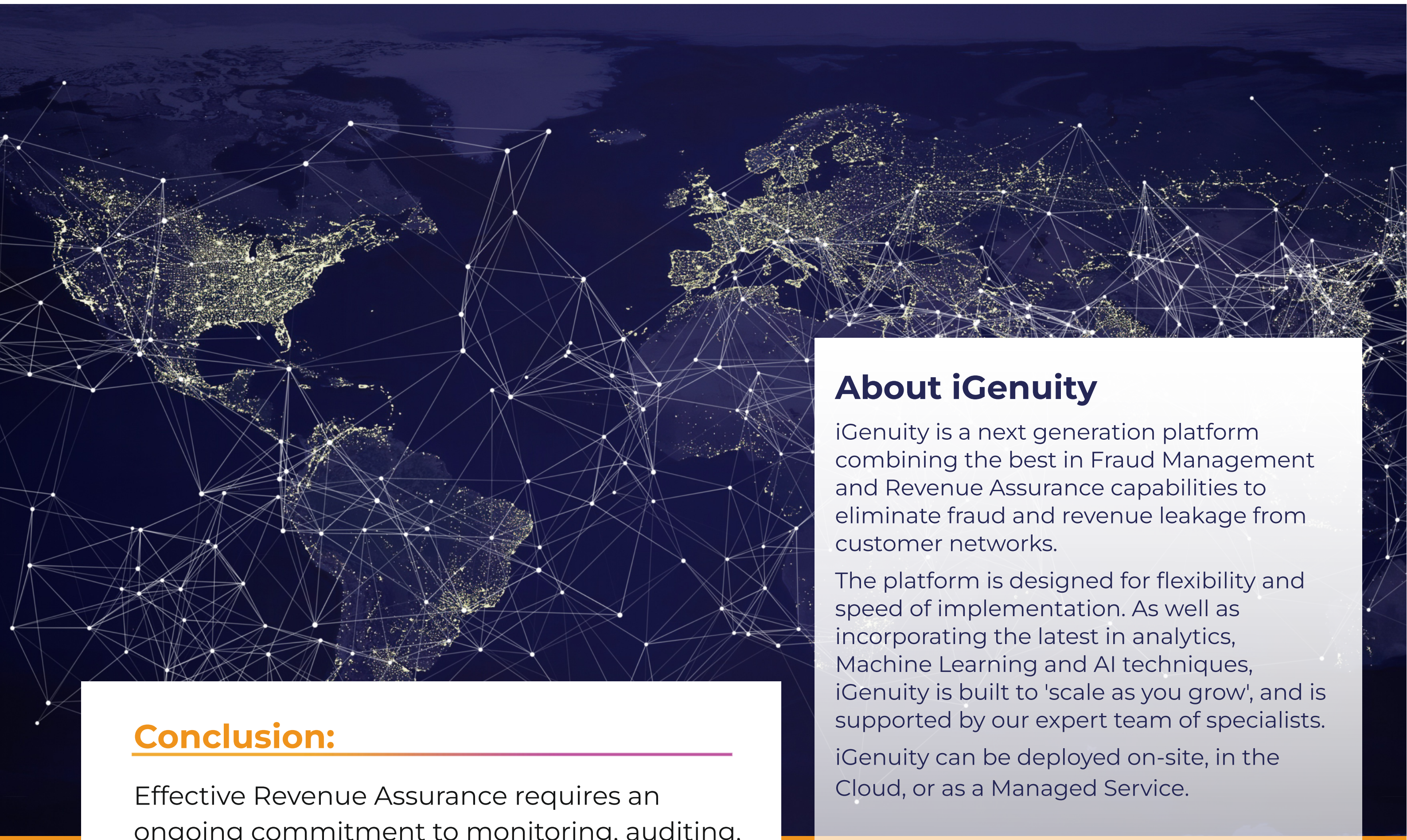
Investigation revealed that the root cause of the issue was a misconfiguration within the billing system by a third-party vendor.

Initially, this had been (falsely) attributed to a database connection issue.

The misconfiguration was corrected, and the problem was resolved.

Key Learnings

- **Simplicity Can Be Deceptive:** Even simple, well-understood processes can harbour critical issues.
- **Importance of Regular Monitoring:** Continuous analysis and reconciliation of event detail records (eDRs) from various network sources would have rapidly identified the root causes of this revenue leakage.
- **iGenuity™:** using the Xintec Revenue Assurance platform, with its robust controls and monitoring, the reconciliation process could have been managed effectively.



Conclusion:

Effective Revenue Assurance requires an ongoing commitment to monitoring, auditing, and reconciling data, even in processes perceived as straightforward.

By doing so, operators can prevent revenue leakage, maintain credibility, and ensure smooth inter-operator billing operations.

Such cases as the one described above underscore the need for proactive Revenue Assurance measures, and the importance of not becoming complacent with seemingly simple tasks.

About iGenuity

iGenuity is a next generation platform combining the best in Fraud Management and Revenue Assurance capabilities to eliminate fraud and revenue leakage from customer networks.

The platform is designed for flexibility and speed of implementation. As well as incorporating the latest in analytics, Machine Learning and AI techniques, iGenuity is built to 'scale as you grow', and is supported by our expert team of specialists.

iGenuity can be deployed on-site, in the Cloud, or as a Managed Service.

Contact Us:

Address Head Office:
5-6 Castle Demesne House, Ivy Terrace,
Tralee, County Kerry, Ireland – V92 Y4DC
Email: info@xintec.com
Office Enquiries: +353 (0) 1 2930260
Assistance hours:
Monday – Friday 8.30 am to 6 pm GMT+1