
Plugging the Revenue Leaks

Published by Ari Banerjee
December 1st 2010

Revenue leakage across a combination of wireline, wireless, and cable services typically ranges at an average from 6 percent to 9 percent annually. As content partner ecosystems continue to flourish within a next-generation network (NGN) framework that now readily gives access to virtually any service, from any platform, and from any place, this range is set to significantly increase – forcing both carriers and vendors acting in a fragmented revenue assurance chain to adopt a centralized strategy.

Managing an ecosystem of 100-plus partners with distinct product sets and features with different pricing and settlement terms creates uncertainty and exponentially increases revenue assurance, fraud, and leakage concerns. With NGN being largely on demand, service providers must be able to account for transactions as they happen. Data must be available in real time, both online and offline, so that root-cause analysis can take place before, during, and after an event. This becomes particularly important in any third-party relationships involving service providers. Only by having this ability can service providers get a full handle on their revenue loss, as well as fully exploit the information to understand and predict up-sell opportunities, customer habits and paying patterns, and potential sources of revenue loss.

It is increasingly important for communications service providers to be able to draw on collected data to gain the required insight in real time. Operators' ability to leverage all the data at their disposal will be limited without an overarching system that can provide access to relevant data, enable analysis of it, and provide actionable reports and insight to end users. As more and more operators' technology teams focus on previously untapped areas – such as discovery of micro segments and divergent populations, social impact analysis, sentiment analysis, the hidden impact of actions and events on customer behavior, detecting sudden behavior change of subscribers and dealers, and margin analytics – it becomes quite clear that use of business intelligence and analytics is steadily becoming a core component of operators revenue assurance strategy.

Since today's revenue assurance strategy crosses different service lines, a holistic revenue assurance strategy needs to consider a few key factors, such as information sharing, process improvement, and above all a clear view of all touch-points. As traffic now routinely crosses any number of different platforms, carriers must be able to view all of these factors while managing every stage of the customer lifecycle.

At the recent [cVidya Networks Inc. Annual User Conference](#) in Barcelona, where I was invited to make a keynote presentation, it became apparent from service providers' presentations that sophisticated pattern-matching solutions need to be incorporated with traditional revenue assurance and fraud platforms. An on-site survey conducted by cVidya – of 76 fraud and revenue assurance managers, representing 60 companies across 35 countries – showed that a majority consider internal fraud a growing concern. Most service providers still perform their internal functional audit manually, which makes it difficult for them to implement any structured process to monitor and preempt this fraud, which tends to remain under the radar.

About 85 percent of the respondents said they are concerned about these unmonitored fraud patterns, pointing to the fact that there is a need for revenue assurance and fraud vendors to provide solutions that will help them to minimize their internal fraud concerns proactively. These results also strengthen our belief that it is time for operators to adopt a more centralized and integrated fraud and revenue assurance strategy. The conference was extremely well attended by operators from across the globe, and it also validated our research that revenue assurance and fraud as software categories continues along an upward curve.

There was a time when operators bought revenue assurance and fraud solutions separately. There were many reasons for that, including vendor solution maturity, different stakeholders managing fraud and revenue assurance in the service provider's environment, inconsistency of processes between fraud and revenue assurance practices, etc. An integrated fraud and revenue assurance strategy will help service providers to plug end-to-end all aspects of revenue leakage and implement streamlined best practices that successfully connect the fraud and revenue assurance domains. I have no doubt that if implemented correctly, an integrated revenue assurance and fraud strategy will be able to plug all aspects of service providers' current and future revenue leakage, from all angles.

(To the original post: http://www.lightreading.com/document.asp?doc_id=200861)