Every telecom business deserves a few "cash cows" to compensate for other slim margin "dogs" in its service portfolio.

Trouble is, the cash cows are constantly jumping the fence to graze in new pastures. Here's some perspective on the issue:

- **Voice mail and other national enhanced services** took off in the 1990s. They cost almost nothing to deliver, yet customers paid several dollars a month for them.

- **Person-to-person SMS and the mobile internet** took off in the 2000s, creating the next wave of premium services.

- However, today with so many services packaged in flat rate offerings, out-of-bundle premium services are scarcer, especially as free, OTT alternatives emerge.

Certainly one service that continues to enjoy premium pricing status is **international roaming**, so it behooves operators to carefully guard that business to ensure it remains profitable and optimized.

Here to explain the business of fine-tuning roaming operations, then, is an expert on the subject, Florian Leeder, Head of Business Unit Roaming at SIGOS.

---

**Dan Baker:** Florian, the enabler of your roaming assurance program is the SIGOS GlobalRoamer service, so maybe that’s a good place to begin.

**Florian Leeder:** Yes, it’s a good place to begin, Dan. SIGOS owns and maintains an international roaming test infrastructure distributed across the entire world — really from all countries to small islands such as Guam in the Pacific to all Caribbean islands. We started to build up this infrastructure called "GlobalRoamer" 15 years ago — today the network cuts across 206 countries across the entire world.
countries worldwide where our probes are installed, enabling operators to use that network 24/7/365 to do their roaming tests, roaming monitoring, and roaming revenue assurance.

Customers such as Deutsche Telekom, AT&T, Telstra or NTT DoCoMo use GlobalRoamer to make sure that their subscriber experience in roaming is inline with the high quality service performance, reliability and quality they demand.

Having access to a global test infrastructure to continuously monitor accessibility and quality in roaming is a key advantage.

The GlobalRoamer Network

It's quite a bit different actually. In carrier testing, you check just a few KPIs infrastructure such as GlobalRoamer, provides the highest value. due to:

- Roaming test is much different because it has gotten more complex over time they should. This is the "early charging" or "late disconnect" problem. e.g. if call durations are manipulated making end customers pay more than long they stay activated. Additionally, carriers usually look into fraud issues called CLI delivery. Both have a major influence if calls are taken and how subscribers can access the services regardless of the country they travel to. This is exactly where GlobalRoamer fits in.

Building up such a large infrastructure and placing test equipment in many countries — and often in preferred roaming locations of various cities — is a major investment to maintain. We think a SaaS model, based on a shared network 24/7/365 to do their roaming tests, roaming monitoring, and roaming contract works and that subscribers can access the services regardless of the country they travel to. This is exactly where GlobalRoamer fits in.

Can't an operator build out its own roaming test network? What's the economic benefit of using the GlobalRoamer?

It's a simple make or buy decision. I think it's the convenience of a service that allows them to get full global coverage without a hassle. Virtually all Network Operators (or Carriers) have roaming agreements in place with something like 200 to 800 other Network Operators across the globe. At the same time, this needs to be tested to make sure that everything agreed to in a roaming contract works and that subscribers can access the services regardless of the country they travel to. This is exactly where GlobalRoamer fits in.

How is roaming testing different from carrier testing?

It's quite a bit different actually. In carrier testing, you check just a few KPIs such as voice quality and if the calling number is represented correctly (so called CLI delivery). Both have a major influence if calls are taken and how long they stay activated. Additionally, carriers usually look into fraud issues e.g. if call durations are manipulated making end customers pay more than they should. This is the “early charging” or “late disconnect” problem.

Roaming test is much different because it has gotten more complex over time due to:

- The growing variety of services; e.g. voice, data, messaging, video etc.

Related Articles

- Nine Simple Strategies for Protecting an Operator or MVNO from Telecom Fraud — interview with Jim Bolzenius — An expert in telecom fraud management explains essential strategies for aiming a carrier’s or MVNO’s fraud prevention program in the right direction.

- A Sweeping 239-Page Research Report on Fraud Management Solutions & Strategies — by Dan Baker — TRI has released a comprehensive analyst report on fraud management solutions. The study is based on interviews with three dozen leading FM consultants and solution experts. Download the free Executive Summary.

- SMS Bypass Blocking: A Service that Protects & Maximizes A2P Revenue for Mobile Operators — interview with Claire Cassar — A2P messaging is a multi-billion dollar revenue stream that mobile operators need to protect. In this interview, you’ll learn how a managed service solution blocks bulk marketing messages and other bypass fraud in enterprise-to-operator SMS traffic.

- Device Intelligence and Big Data Linkage: Guarding Consumer Access Points from the Fraudsters — interview with Matt Ehnich — Preventing subscription fraud today means supplementing traditional identity checks with a host of new processes, technology, and big data analytics. A credit and fraud risk expert explains the roles of predictive scores, device risk assessment, and linkage analysis.

- Mapping the Interconnect Resale Routes of Fraudsters: How a Global Robot Network Detects Voice and SMS Bypass — interview with Xavier Lesage — SIM box voice bypass is a persistent problem, but now, bypass is spreading to SMS, OTT apps on the smartphone, and ghost trunks. This interview explains the fast evolving bypass scene, highlights the strategy of fraudsters, and provides case studies.

- Law Enforcement & Security in a World Where Industry and National Boundaries are Blurred — interview with Mark Johnson — Are we destined to be forever reactive over security, fraud, and risk issues? Or will we put wise standards, regulations, and frameworks in place that allow us to deliver technology that’s relatively secure and fraud-resistant?

- Thinking Outside the Comms Box: A New, Cross Industry Fraud Check Service that Telecoms can Leverage — interview with Jim Rice — For decades, telecoms have done fraud and identity checks using comms industry data. This interview explains the power of using cross-industry data to pinpoint known fraudsters and suspicious individuals in finance, retail, and other industry data sets.

- Integrated Test Call & CDR Analysis: A New Tool in the Fight Against SIM Box & OTT Bypass Fraud — interview with Kenneth Mouton — Why not combine the
as well as 3 different technologies today: GSM, UMTS and LTE;

- The introduction of special roaming packages and other solutions to allow subscribers to keep their costs under control;

- Data-hungry smartphones that serve many applications with real-time information is another big issue; and,

- Last but not least, voice is transforming into an IP application.

So all these factors have brought challenges to roaming. It’s about new technologies in the field, new libraries, and new use cases that all need to be verified, tested and supervised over time.

SIGOS GlobalRoamer customers simply subscribe to our service and access the Global Roamer network via a web based GUI to run their own tests. Or if the operator prefers, we have expert consultants in Germany and Belgium who do all the testing on their behalf. And, of course, they are there to help with troubleshooting too: roaming is complex, LTE roaming is complex, and so is roaming billing. So you need domain knowledge to understand the traces and the potential problems. Plus errors need to be fixed fast!

One area where operators certainly need roaming test is around roaming arrangements for LTE. What’s happening there, Florian?

SIGOS is supporting network operators worldwide to build up and successfully launch international LTE services. The expertise and the test methods we developed with operators, plus keeping up with industry standards in roaming is also key. In 2012 we rolled out the first LTE and CSFB test locations with GlobalRoamer. Today we offer LTE technology in over 80 countries, well ahead of market penetration at this point.

Operators, of course, implement LTE in their home markets and stepwise start to negotiate roaming agreements with their partner networks. That’s what’s going on right now. Roaming using totally new network technology creates a high demand to test, measure and troubleshoot problems. Many things change and it all needs to be managed both: contractually between operators and technically to provide reliable and high quality service.

We actually help operators across the board with LTE. We not only consult with them on the technical and billing details, we also help them negotiate deals with other operators.

For instance, customers might approach us and say, “Look, my marketing department says I need 100 LTE roaming agreements by the end of the year. But I only have five people on staff, so can you help?”

And of course, we use the GlobalRoamer network to do all the international testing from one location. The process starts simply by engaging with the desired list of roaming partners, then moving to contract and price negotiations.

The technical part comes next: SIM cards are exchanged to execute real tests. For instance if we act as agent of KPN and are negotiating with T-Mobile USA, then T-Mobile USA sends us SIM cards that we use to test in the Netherlands. Likewise, KPN sends their SIM cards so we can test those in the US and so on.

However, even after a successful functional testing, you’re still not ready because you’ve got to ensure billing is correct. So we check our CDRs to make sure the right tariffs have been applied. Only when this “TADIG testing” is successful is a commercial launch letter prepared. And when both parties sign virtues of FMS CDR analysis and test call generators to create a single integrated tool for bypass fraud control? The benefits of that idea, a tutorial on test call systems in SIM box detection, and OTT bypass via mobile services like VIBER are all discussed in this interview.

- White Paper: How to Defend Your Network Against the New SIM Server Threat — by Dan Baker — SIM box bypass is a very stubborn fraud problem: fraudsters are succeeding despite carriers’ best efforts to defeat the fraud. This white paper explains the impact of SIM Servers as a powerful stealth weapon of the fraudsters. In turn, the paper discusses new technologies and strategies that can defeat the more sophisticated types of SIM box fraud emerging.

- Intelligent Routing: The Case for Blocking IRSF Fraud at the SIP Session Border Controller — interview with Michelle Wheeler — Analytics data today is managed in a privacy-negligent way. This interview discusses an ingenious privacy and analytics exchange that allows telecoms, banks, and money lenders to trade fraud, credit risk and other data with each other in complete confidence and control.

- A Privacy-Enabled Data Exchange that Expands Analytics Uses in Fraud, Credit Risk and Beyond — interview with Shankar Panianandy — Adaptive and behavioral learning systems are at the forefront of R&D in telecom fraud management systems. Here an expert developer explains their usefulness in use cases such as IRSF detection, subscription fraud, application fraud, and voice biometrics.

- Protecting 900+ MVNOs around the Globe from IRSF Fraud Pirates — interview with Colin Yates — Telecom fraudsters are seeking a new, more vulnerable path to riches. Their target: 900+ MVNOs around the globe who generally own no mobile networks, but sell mobile service virtually. This interview with a fraud control expert explains what steps MVNOs must take to protect themselves from IRSF fraud.

- Insider Fraud: How to Create an Anti-Fraud Culture in Your Telecom Organization — interview with Mark Yelland — Thirteen years after the WorldCom scandal, experts generally agree that insider fraud remains a massive problem in telecom. In this article you’ll learn the outlines of building a program to instill an anti-fraud culture at your telecoms organization.

- IRSF Protection: Software that Blocks Telecom Fraud at the Enterprise PBX — interview with Roger Ansin — The richest criminal path to International Revenue Share Fraud (IRSF) goes through the enterprise PBX. Hijacking the PBX has cost businesses and telecoms countless billions of dollars in the past 15 years. In this interview you’ll learn about this industry challenge and an affordable and proven tool that blocks IRSF at the enterprise.

- Combating SIM Box Fraud: Network Protocol Analysis to the Revenue Rescue — interview with Lex Wilkinson — International call bypass is fraud perpetrated through SIM boxes equipped with dozens to hundreds of SIM cards that disguise international calls as local domestic phone calls. This article give a background on SIM box detection techniques and talks about a new, rapid-detection technology based on network protocol analysis.

- Making the Retail Operator Case for Anti-Fraud Protection via Wholesalers — interview with Jan
off on that, roaming is in place and the project moved to the next step to observe the quality level for the months and years to come.

What network problems do operator typically run into when roaming is not working right?

There is a number of typical problems but let’s take one that is surprisingly common.

Let’s say you are a customer of Vodafone, and your operator provides you excellent LTE services across your home country. When you travel abroad, your phone is looking for the same network technology, so it will look for a LTE network in your roaming destination.

What we often see is that the LTE network is not configured correctly in cases where LTE roaming is not in place. Instead of replying with “LTE network is not available” it reverts to the message “network access not allowed”. The effect of this, unfortunately, is that the user is now also excluded from GSM or UMTS services of this network. So in the worst case, the user has no network connection at all.

Regulators in the European Union (EU) have been putting on the pressure over bill-shock and roaming fees. What’s the status of these regulations?

Well the regulation has gone through various stages. At first, the EU implemented some price caps on the retail market: the wholesaler side has not been regulated.

Then, in an effort to create more competition, they opened up the market to players outside the mobile operator space. So companies like the airliner Lufthansa can now offer roaming services, however, so far the pick-up is very, very slow.

Why? Well, one reason is that the EU threat of further price regulation forced operators to cut their prices. Another big factor is the availability of WiFi. People who traveled abroad got “bill-shocked” and lost confidence in mobile data roaming, so they switched data roaming off and started using WiFi instead.

In other words, a strong business case isn’t there for new roaming players to enter the market as Roaming charges went down already.

Of course, we’re still waiting for 2017 when the “roam-like-home” law will be in force, meaning Roaming charges will be banned in Europe (EU) — subscribers will pay the same price as in their home network.

So what’s the impact going to be?

Certainly if operators earn less money from roaming, it could have a big impact. It would mean that roaming will no longer be a premium service for operators.

On the other hand, I am not too concerned, because there is a very high number of so-called “silent roamers” out there. Lower prices will dramatically stimulate the market and silent roamers will turn on their data roaming
Protecting the International Roaming Cash Cow: Using a Global Test Network Service for LTE Deployments & Beyond

The accompanying chart shows the behavior that one of our European customers is forecasting when the “roam-like-home” is in place. Today only 30% of the operators subscriber base is using roaming when abroad, and the ones who do roam consume only 40% of the volume they consume in their home network.

Great, Florian. Excellent briefing. The roaming glass looks like it’s only 35% full. Given some creative pricing and marketing, there’s a revenue upside that operators can enjoy.

Copyright 2015 Black Swan Telecom Journal

Share via facebook.

Two clicks for more privacy: The Google+ button will be enabled once you click here. Activating the button already sends data to Google – see i. not connected to Google+

Two clicks for more privacy: The Linked in button will be enabled once you click here. Activating the button already sends data to Linked in – see i. not connected to LinkedIn

Send this via email to a friend.

Two clicks for more privacy: The Tweet this button will be enabled once you click here. Activating the button already sends data to Twitter – see i. not connected to Twitter

If you activate these fields via click, data will be sent to a third party (Facebook, Twitter, Google, ...) and stored there. For more details click i.