Revenue Assurance: A Matter of Survival!

Sérgio Braga	Sérgio Pereira	Oclair Prado
(sbraga@cpqd.com.br)	(sergiop@cpqd.com.br)	(oclair@cpqd.com.br),
Business Analyst	Cellular Market Manager	Systems Analyst
Fundação CPqD	Fundação CPqD	Fundação CPqD
(www.cpqd.com.br)	(www.cpqd.com.br)	(www.cpqd.com.br)

Abstract.

In this paper we'll show the main points where we usually find revenue leakage in Telecom companies and the actions that may be taken in order to avoid this kind of loss. We'll also identify, within the "revenue cycle", the most appropriate points to be monitored by the existing Verifying and Controlling Systems.

Another objective of this paper is to classify some systems built for "Revenue Assurance" with TOM (Telecom Operations Map) [1].

Key words.

Revenue Assurance, Net Management, Revenue Cycle

1. Introduction

The attention dedicated to Revenue Assurance today reminds a little what happened with the Y2K all the way through 1990s [2]. In the early 1990s, just a few people were concerned about that problem and the systems repair cost was equivalently low. By the end of the decade, this problem increased making many people worried about it and therefore systems repair cost became astonishingly high!

Certainly "revenue leakage" has existed in Telecom companies for a long time but only in recent years, this matter has received a great amount o interest. Maybe because of recent publications showing annual losses around R$ 2.48 billion [3] in companies only in Brazil during the year 2000. The companies' Top Management have just started paying attention to this matter recently, when they have realized that their companies have been losing from 3% to 11% of their revenue and in some critical situations this rate may reach 15%!

Some companies have just started their actions towards this direction but they are mainly worried about the stream "switch – mediator – billing" and are leaving other streams with no

care at all. As we are going to in the section “3 – Control Points for Revenue Assurance”, there are several systems that may be used to monitor and control revenue leakage such as the “Volume Trending” and “Supervision” ones.

2. Revenue Cycle

“Revenue Cycle” enumeration and classification may be as large and detailed as one wishes. In this paper we’ll present a suggestion for this cycle and we’ll emphasize some places where revenue loss are more frequently found and hence more likely to happen.

In figure 1 we can see an example of some processes involved in one phone call from customer A to customer B that are in different Local Carriers ranges.

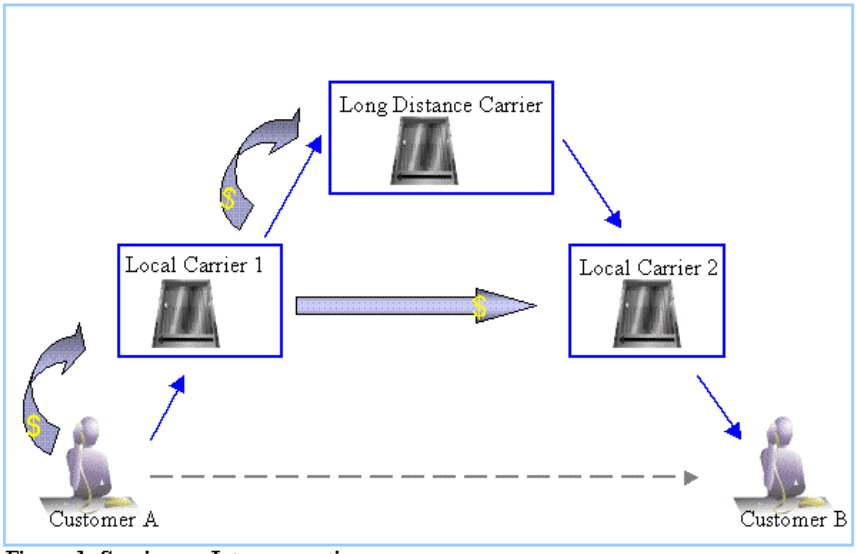

Figure 1: Service vs. Interconnection

Their conversation is possible because there are interconnection agreements among local carriers and long distance carriers. We can see in figure 1 that a call not billed by the local carrier 1 means practically double revenue loss. The customer A will not pay it but it will be paid by local carrier 1 to the other local carrier and to the long distance carrier according to their interconnection contracts [7]. The reasons why Local Carrier 1 doesn’t bill some calls will be discussed in the next section of this paper.

In figure 2 we show some components of a Telecom Company Revenue Cycle and we highlight the places where we frequently find revenue leakage.

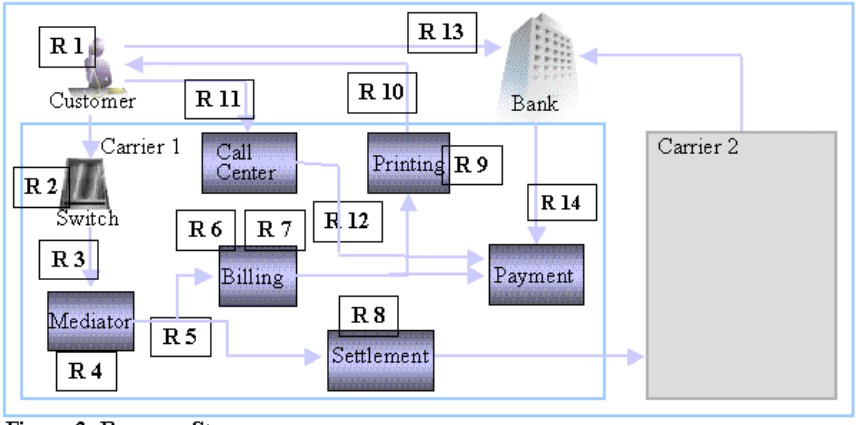

Figure 2: Revenue Stream

R 1. Customer uses the service, plan or package (the beginning);

R 2. Switch generates the record (CDRs or others);

R 3. Mediator collects the switch records;

R 4. Mediator validates the records and builds the files with them;

R 5. Mediator sends the files to other systems (Billing, Settlement, Performance Net Manager, Fraud and others);

R 6. Billing system reads the files and prepares the records;

R 7. Billing system rates the records;

R 8. Settlement system processes the records to bill other carriers;

R 9. Carrier prints the customer bills with the available Billing system data;

R 10. Carrier sends bills to the customer;

R 11. Customer complains about something on his bill;

R 12. Call Center gives discounts directly to customer bill;

R 13. Customer pays his bill through a bank;

R 14. Bank sends the amount paid to carrier;

In all of these items we may have revenue loss and in the next section we will be discussing the main control points for revenue assurance. We will show that Revenue Assurance contains Revenue Cycle and some other carrier's administrative processes.

3. Control Points for Revenue Assurance

The control points for Revenue Assurance may vary a lot from one carrier to another. In this section we will present some of the main control points and the most frequently problems associated with them. We also show some systems frequently used in order to monitor them.

The low amount of monitoring systems in use for this purpose in Telecom Companies is amazing. Compared to banks, the verifications done by telcos are almost nil [6]. It is not surprising that they are losing so much money. They have not realized yet that they are sending money through their systems instead of data only.

In figure 3 we're presenting a suggestion for the main control points for revenue assurance.

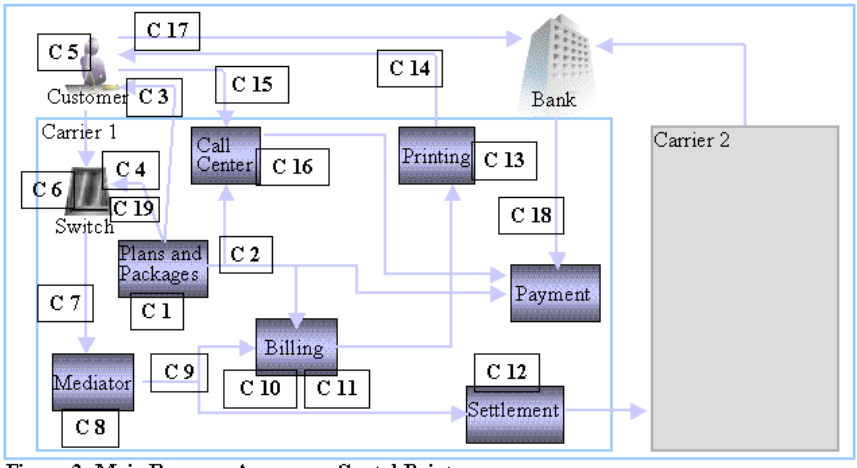

Figure 3: Main Revenue Assurance Contol Points

C 1. Carrier builds new plan, service or package;

In this point the carrier may lose revenue when it cannot follow their rivals or when it cannot accomplish its own plans. The customers may cancel their contracts and migrate to other carriers (churn).

C 2. Carrier prepares its systems and records to accomplish the previous point;

When the carrier loses synchronism between both, new service that have just been launched and its systems records, it will certainly lose revenue. To avoid this kind of problems, telcos may use "verifying" systems that will be discussed in the next section of this paper.

C 3. Carrier sells its new service, plan or package to the customer;

Here the loss occurs mainly because of customer fraud. Some bad intentioned customers buy the new carrier services using false documents and just disappear after some time, leaving their bills behind with no payment. For this kind of problem the solutions are known for a long time and are shown in the next section of this paper on item Fraud (F).

Another relevant factor here is that carriers usually don't have cost control systems or they don't use them when they are planning new services. They rarely know their costs and, for this reason, they don't use this information when they are making their prices.

C 4. Carrier does the provisioning at the switch;

The more common problem here happens when the carrier sells its short period promotions. Without a well-controlled process, this period may last forever. Another problem usually faced here is the great amount of lost lines or test lines installed in customer residences. All these problems may be monitored with "verifying" systems with great efficiency.

C 5. Customer uses the service, plan or package (the beginning);

The more common leakage in this item is the clandestine calls made on public telephones. Cloning cellular telephones fell from 4% in analog telephones to less then 1% in digital ones. The "fraud" systems are used to fight this kind of loss.

C 6. Switch generates the record (CDRs or others);

In this point it is necessary to separate the problems in two main classes:
(a) the software based ones that occur when switch tables are not synchronized with the carrier. A frequently found problem is the switch routing table with older information than the carrier;

(b) the hardware based ones that usually happen are caused by a short-circuit in the switch or other kind of switch circuit mal-functioning.
Great amount of bad CDRs is generated without time duration or initial call date or other similar faults that invalidate these CDRs for billing. These bad CDRs are created because of software and hardware problems. When a customer makes his call without its corresponding CDR, the carrier loses revenue. There are systems that automatically test switches in order to verify if they are generating all kinds of CDRs correctly. Carrier must repeat these tests very frequently, at least monthly or when switches' version system is altered.

C 7. Mediator collects the switch records;

Problems may occur when files are transmitted from switches to mediator. A way of avoiding this problem is to use a "volume trending" system as described in the next section of this paper.

C 8. Mediator validates the records and builds the files with them;

When the mediator validates the CDRs to create the files, some business rules have to be used. When these business rules don't cover all the possible situations, some CDRs will probably be discarded as bad ones. In these cases we will have the same considerations done in point number 6. The mediator must be checked very frequently to certify whether it is able to deal with all necessary kinds of CDRs. In this point the "verifying" systems to validate the records used along these processes in the mediator, especially routes, prefix numbers and files deliveries may also be used.

C 9. Mediator sends the files to other systems (Billing, Settlement, Performance Net Manager, Fraud and others);

Here we may repeat what was stated in point 7.

C 10. Billing system reads the files and prepares the records;

The most frequent reason for revenue loss in this point is the absence of synchronism between billing records and other carrier's systems records. To help in this point we may use "verifying" systems too.

C 11. Billing system rates the records;

Again the record problems are the main reason for the leakage in this point and the considerations of the previous one are also applicable here.

C 12. Settlement system processes the records to bill other carriers;

The most important problems here happen with the interconnection contracts not well negotiated or not sufficiently clear and bad route records and not updated prefix numbers. This is an item of great interest because it is responsible for almost 30% of local carriers' revenue and the problems here tend to grow with the coming "unbundling". The "verifying" systems will be of good help here in record analyses. Another problem that may affect this control point is the lack synchronism of the switches' watches. It is possible to lose CDRs or bills in double because of synchronism problems in switches' watches.

C 13. Carrier prints the customer bills with the available Billing system data;

Periodical and thorough checking process to certify that all bills are printed and sent in time to be paid is necessary. A bill received with some delay will upset the customer and increase churn risk.

C 14. Carrier sends bills to the customer;

We may repeat here what was stated in the last control point.

C 15. Customer complains about something on his bill;

Recent statistics show that 80% of calls made to Call Centers are from customers that do not pay their bills with carrier's authorization. This problem may grow by fraud or customer short cash problems.

C 16. Call Center gives discounts directly to customer bill;

These problems get bigger when Call Centers give unauthorized discounts to customers.

C 17. Customer pays his bill through a bank;

The revenue leakage occurs when the customer doesn't pay his bill or doesn't pay it on time.

C 18. Bank sends the payment to carrier;

A common cause of revenue loss in this control point is the excessive delay that may occur in the process of sending the money from customer bill to carrier. This money may not even be sent to carrier when a problem with bank records occurs. Bank records must be verified regularly.

C 19. Carrier cuts off services of delayed customer's switches.

The records don't stay as expected by the carrier forever. A dismissed employee is able to alter record information or the *jumps* in the switch. The carrier systems sometimes make lines reservations that are never used and these unused lines don't generate revenue. The "verifying" systems are also welcome in this control point.

Note that points from 5 to 18 are the same as Revenue Cycle points from 1 to 14.

4. Classification of some kinds of systems used in Revenue Assurance

Nowadays solutions are built with many kinds of systems:

- Specialized Audit (A)

A high-qualified professional should execute the switch tariff checking. This process consists of a large range switch audit in which the settings and internal status are verified. This professional usually has many years of experience and knowledge that help him detect and correct switch problems and even in the company's internal processes.

- Automatic Call-Through Tests (AT)

The central office switch contains necessary information to rate, route and record a call properly. This translation information is stored in tables and changes frequently as new customer lines are provisioned or service is changed. The dynamic nature of the translation tables poses a challenge for network reliability groups. This kind of system makes calls, logs the results and compares it against the AMA (automated message accounting) for billing purposes [8].

- Supervision (S)

Nowadays this system class is the most common in use. Network Management group usually uses it. Through the Performance Indicators generated, Network Management groups are able to detect and correct the problems in their networks. The systems which monitor files transmission from switches to billing, passing through mediator, that generate alarms when a missing file is detect also belong to this class. It is normal to insert these systems in the mediation solution.

- Records Verifying (V)

The Revenue Assurance Control Points overview shows that in more than 50% of them, revenue leakage is caused by problems with the companies' records. Because of its high impact in the revenue cycle, this kind of problem should be the first one to be dealt with but not the unique. Recent studies show that this system class acquisition usually pays itself after a few months just with the recovered revenue. Since record problems are dynamic, this software class cannot be stopped otherwise the problems will come back bringing equivalent revenue loss.

- Volume Trending (T)

This kind of system captures the actual switch call volumes and stores them in a history database. Once there is enough historical information to evaluate, expected volume ranges can be set. Management then has to decide what the acceptable fluctuation range will be.

Exception alarms will be generated and sent when switch volumes fall above or below bounds established by the user [9].

- Fraud (F)

This is the oldest kind of system used for this purpose and the more common still in use. They usually work like trending systems, which build their knowledge base with their user's behavior and take their actions after detecting abnormal variations.

5.CPqD's Systems for Revenue Assurance Classification with TOM (Telecom Operations Map)

Figure 4 shows some CPqD's systems for Revenue Assurance classified in "TOM – Service Provider Processes".

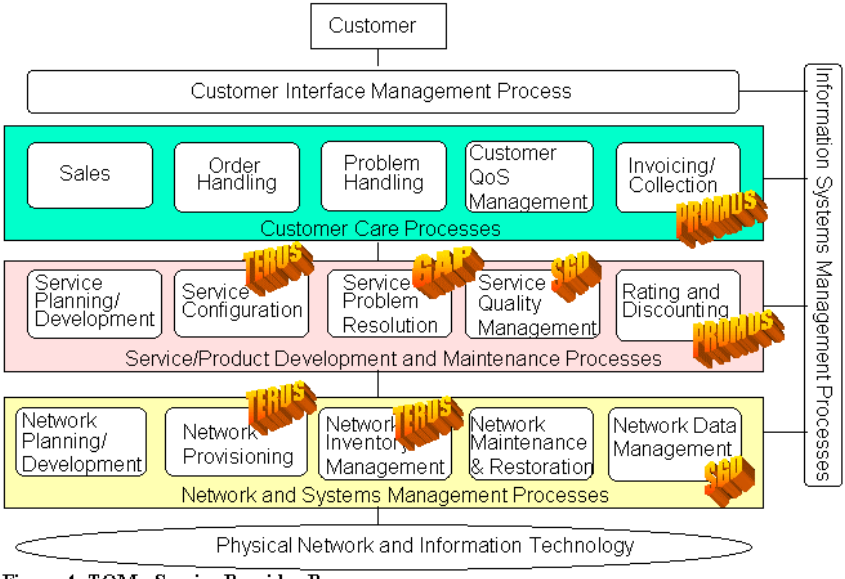

Figure 4: TOM - Service Provider Processes

TOM consists of:

- A high-level, static view of Telecommunications Operations processes and sub-processes that is top down, customer centric, and function based;
- A high-level "skeleton" that illustrates the primary end-to-end processes of fulfillment, assurance, and billing, and identifies sub-processes within each;

- A dimensional approach to understanding the functions involved in certain Service Provider deliverables;
- Illustrative examples of process flows that show end-to-end process;
- A more detailed view of the functions of each sub-process, including functions or activities of each sub-process box, as well as its inputs and outputs to other sub-process boxes.

Based on this guide we'll present these systems classification and processes used at this moment for Revenue Assurance by CPqD and other Telecom Service Providers.

1. Terus.

   It is a "verifying" system. It does switch data audit and compares the collected data with SSO, Billing, CRM and other company systems data available.

2. Switch Audit.

   It is an "audit" process. A high-qualified professional should execute the switch tariff checking. This process consists of a large range switch audit in witch settings and internal status are verified.

3. GAP Analysis.

   It is a "volume trending" system. Actual CDR volumes are captured from switch and stored in a history database. Once there is enough historical information, expected volume ranges can be set by the user. Management then has to decide what the acceptable fluctuation range will be. Exception alarms will be sent when switch volumes fall above or below bounds established by the users. Even if no alarm is generated, a daily report about the amounts analyzed during the day may be created, saved in its database for further use, and sent to the users.

4. Net Performance Management System (SGD).

   It is a "supervision" system. It generates Quality Indicators based on CDRs and some Performance Indicators that together with Call Completing Matrix may point net problems and show where the critical ones should be or are more likely to happen.

5. Promus-Settlement.

   It is a "verifying" system too. This module analyzes the CDRs, routes and, based on the interconnection contracts, calculates the amounts to be paid and to be received by the carriers.

6. Conclusions

We believe that the Revenue Leakage in Telecom Companies tend to be minimized in the near future. Some recent facts point towards this direction, such as the growing interest manifested by he managers about this matter and the creation of new departments exclusively to deal with it. Besides that, the use of specialized consulting to help the detection of these kind of problems and also to suggest corrections or recommend systems acquisitions to automatically monitor the control points of revenue assurance that generate alarms in critical situations is even more frequent.

TOM adoption as a blueprint for telecom systems and its interfaces is also helping to reduce the Babel of systems. These “Frankensteins” help a little or even introduce more confusion in the scenario becoming a potential source of revenue loss.

7. References

[1] Telecom Operations Map, GB910, TeleManagement Forum 2000, version 2.1, mar / 2000

[2] First Revenue Assurance Survey, Deloitte & Touche, http://www.us.deloitte.com/pub/revassur/revassur.htm, 1998

[3] Vazamentos Bilionários, Teletime 4-29, http://www.teletime.com.br/revista/29/capa.htm, fev / 2001

[4] On the Front Lines: PWC Survey Telecom Professionals on Revenue Assurance, Billing World, http://www.billingworld.com/full.asp?id=1895&action=article, nov / 2000

[5] Wireless Revenue Assurance, Billing World, http://www.billingworld.com/full.asp?id=1892&action=article, nov / 2000

[6] Revenue Assurance at the Switch, Billing World, http://www.billingworld.com/full.asp?id=2067&action=article,jan / 2001

[7] Considerations for Outsourcing Revenue Assurance, Billing World, http://www.billingworld.com/full.asp?id=2054&action=article, dez / 2000

[8] Moving Upstream in the Revenue Assurance Pipeline, Billing World, http://www.billingworld.com/full.asp?id=774&action=article, jun / 1998

[9] Putting Revenue Assurance into Practice, Billing World, http://www.billingworld.com/full.asp?id=590&action=article, jan / 1998

8. Acknowledges

The authors would like to thank CPqD for permitting this paper publication with practical results achieved in this area and information about some systems for Revenue Assurance.