# Adaptive Revenue Assurance Delivers Maximum Network Profitability

## Understanding and stopping revenue leakage helps service providers reduce operating costs and increase profitability

Innovative revenue assurance solutions such as the Lucent *Navis*® Revenue Locator offer huge potential revenue gains with ROI achievable in months.

**This white paper addresses how to:**

- Identify causes of revenue leakage in the network
- Evaluate the different tools available to stop revenue leakage
- Deploy Adaptive Revenue Assurance systems in your network
- Turn revenue losses into profits with *Navis*™ Revenue Locator

Lucent Technologies
Bell Labs Innovations



## Introduction

Revenue assurance, actively seeking out the sources of lost income from network operations, is an area that was nearly unexplored two years ago. The focus in the area of revenue loss has traditionally been fraud detection and management. Today, nearly all service providers are focusing on revenue assurance: today's economic pressure to maximize profitability and reduce costs may be the primary reasons. Another reason may be the diminished emphasis on capturing new market share—3G deployments are being delayed; new "killer" applications in the wireline space are not fully available either. This shifts the focus to optimizing profitability within the provider's existing market. Whether the concentration on revenue assurance is driven by economics or technology, one thing is clear: the potential benefits are huge, and advanced solutions are available that provide return on investment in months.

Studies* (which) indicate that Service Providers lose a minimum of 2-5% of their annual services revenue due to services that were never billed, and in some cases as much as 15%! Revenue leaks occur at different stages of the billing process, from a customer's ordering the new service to the provider making network switch changes and establishing accurate billing records reflecting the change. In addition, worldwide annual telecom losses due to fraud are estimated at US$ 14 billion. Fraud has been a focus area for every service provider already for decades. Fraud and other revenue leakage will need even more focus in the future. Looking at the impact of new high-value services in technologies, such as 3G, the potential revenue loss per minute will be drastically higher than the potential loss per minute from 2G services. If more data usage is billed per minute, the potential becomes greater for more to be "unbilled".

## Understanding Revenue Leakage

Total revenue losses (of the 2-15% mentioned above) can be separated into several categories, that help to better understand leakage (Figure 2). For post-paid services, close to 50% of the revenue loss is due to network and mediation-related issues, such as incomplete records, parsing errors, etc. About 18% is due to fraud, about 25% related to billing and revenue collection and 11% related to provisioning and order management.

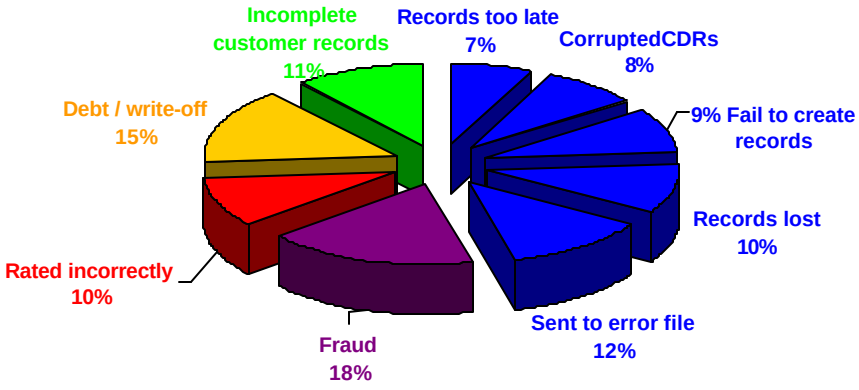


**Figure 2:** Sources of revenue leakage: nearly half of revenue leakage is network-related.
**Source:** The Phillips Group 2001

This is not a new concept to most service providers. Leading service providers have been looking into revenue assurance over the past few years. A first step usually involves consultancy audits to understand specific network and billing operations. As a next step, dedicated resources are hired to work on closely defined revenue assurance projects. In most cases this revenue assurance department reports into the CFO department. Some operators have decided to align part of the revenue assurance resources with the network operations department—perceived by some as a better choice for focusing on network-related issues.

Network-related leakages are not easy to detect, especially in light of today's network complexities. A single service typically uses a wide set of technologies, often involves other parties such as applications developers and even direct competitors. This is a challenging environment in which to analyze network data and increases the difficulty of making unanimous decisions about what is causing the leaks and what needs to be fixed. Because of the dynamic nature of today's networks, and the services being offered, as leakage is found and corrected, new points of leakage may develop and outpace the ability to find and correct them.

Accordingly, detecting and correcting network-related leakages can become a monumental, seemingly impossible task involving processing millions of data records from diverse sources to find discrepancies. Furthermore, it often involves the collection of data from multiple points in the network—from network elements, from probes, from mediation and even from billing systems—and a comparison of all these records in order to find "lost" or incorrect data.

## Tools to Stop Revenue Leakage

There are several approaches to the challenges of finding and stopping revenue leakage. These approaches combine physical processes, automated systems and skilled people. Previously, the focus on solving revenue loss problems centered on establishing a small, reactionary team of subject matter experts dedicated to tracing one specific problem out of many. This very costly investment with limited savings potential concentrated on one problem area only and did not address the prevention of new areas of leakage. Employing permanent teams of dedicated processes may also bring improvements, but drastic decreases of revenue leakage will still require more sophisticated, automated and adaptive testing and analysis tools.

***A number of tools—suitable for supporting revenue assurance projects—are available on the market today. They can be grouped into three main categories: reporting, testing and analysis tools.***

### *Reporting Tools*

All service providers use revenue-reporting tools of some sort to generate daily, weekly, or monthly financial and usage reports. Reporting tools, are very useful for tracking service usage over a given period of time, total usage by account, etc. To a certain extent, reporting tools can also help detect revenue leakage, but only when they have reports designed for this purpose. To a large extent, only a limited set of the network-related issues can be uncovered by these reports based on the data that is typically tracked.

### *Testing Tools*

Testing tools are designed to verify that a new service is correctly billed prior to launching the service on the network. These tools, while able to verify billing performance in a controlled trial environment, are insufficient to guarantee minimal revenue loss in a fully operational environment. Trials only permit you to see the results of the specific test cases— operational leakage, such as provisioning and activation errors that can lead to leakage can be missed and left uncorrected when the services go live.

### *Analysis Tools*

There is a clear difference between tools that help you analyze data and tools that generate reports. When seeking an analysis tool, you may really get an explanation about the capabilities of a reporting tool. However, there is a clear difference between tools that help you analyze data and tools that generate reports. Analysis tools are interactive, and enhance and clarify the data visually while you point and click. Reporting tools are not interactive. They just show you a set of pre-defined reports, or generate a new report after you define the new output you want. It is much easier and faster using analysis tools to find revenue leakage.

## Adaptive Revenue Assurance

The ultimate tool for revenue assurance purposes should detect revenue leakage automatically. It should detect leakage based on the real services used in the live network, not based on test calls. The tool should analyze the data in real-time and prioritize the leakage cases, so that operators can immediately focus on the most important leakages. Most importantly: the perfect revenue assurance tool should be *adaptive.* This means:

1) It should not require any rules to be set up to detect revenue leakage
2) It should automatically learn from the network at initial setup as well as adapt its behavior as the network evolves.

This adaptive performance is the only practical way to find revenue leakage efficiently in today's complex networks.

Why are non-adaptive tools becoming obsolete? Because non-adaptive tools require experts to define a set of rules to detect leakage. Non-adaptive algorithms were the basis of most fraud detection systems in the past. Once you know what type of fraud is happening, you can define a new rule and be warned immediately when this type of fraud happens again, and thereby stop the fraud. This works fine, as long as it takes a while until this type of fraud spreads in the network. However, with today's Internet communication, any news is spread in minutes. It takes only one person to post a trick how to commit fraud on the web, and you are losing a lot of money immediately. Non-adaptive fraud systems also assume that you are aware of this fraud vulnerability in the first place—and you are capable of defining a rule to capture the case.

Adaptive tools analyze network behavior and detect, prioritize, and alert you to revenue leakage as soon as it becomes significant. No rules need to be defined—the system will learn from the network and adjust its behavior as the network changes. Since adaptive tools don't require any specific setup, they are not only able to monitor what happens within your network, but also what happens in your partners' or competitors' networks. Why? While network are so complex that no human can still understand the complete network setup, the network does understand itself—as it is able to provide end-to-end service. Whether a call originates from your network, terminates in your network, or flows through your network, your network has information about this complete or incomplete call. When the adaptive tool processes the information related to this call, it can detect issues, even when the issue itself is in your partner's interconnect network. Field trials with adaptive tools have proven that this works. Wouldn't it be great to know that you can increase your revenue by asking your partner to fix a problem for you?

There is one caveat when using adaptive tools for detecting and alerting on revenue leakage. The system—and not you—understands this leakage. The system has the intelligence. It processes millions of data records to alert you that there is a potential leakage. The system may very well generate a report on the leakage it found, but how will you understand that report? How do you get from adaptive revenue leakage detection to knowing what to fix in the network? It requires an innovative visualization and analysis tool that can show multiple dimensions of data on one screen, and that instantaneously changes how the data is shown by simply moving a pointer over the data (Figure 3). This analysis tool should be able to depict hundreds to thousands of data records in a dynamic way, so you can understand the leakage in a few minutes, and get the leakage stopped within the next hour.

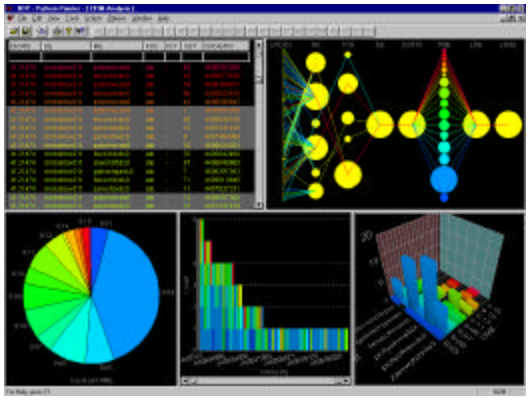

**Figure 3:** Example of an innovative analysis tool for locating revenue leakage, developed by Bell Labs for Lucent Technologies.

## Turn Revenue Leaks into Profits with *Navis*® Revenue Locator

With the increased complexity of networks and services, it becomes impossible for a single human being to understand how the network really works. While non-adaptive fraud detection systems were capable of keeping losses due to fraud under control in the past decade, no one will be able anymore to configure non-adaptive revenue assurance tools in a timely manner. Today's revenue assurance tools have to be adaptive: they have to learn from the network, and adapt themselves as the network evolves. Adaptive revenue assurance tools, together with innovative visualization and analysis tools, will enable service providers to be alerted on, analyze, and finally minimize their losses due to revenue leakage by getting issues resolved within minutes or hours.

Lucent Technologies *Navis*® Revenue Locator is a leading software solution that delivers the adaptive revenue assurance results that Service Providers require. It allows them to be alerted of revenue leakage in real time. It further allows operators to perform detailed on-demand analysis in order to identify the cause of the leakage. Up to 50% of leakage problems can be detected and analyzed with *Navis*® Revenue Locator.

Is an adaptive analysis tool a good investment? The business case is very simple. With a subscriber base of 5 million units and a yearly ARPU of $200, revenue leakage sums up to $20-50 million per year. With a tool like the *Navis*® Revenue Locator, a Service Provider might locate leakage that could potentially add $10-25 million to their bottom line, every year. Given this scenario, the potential return on investment (ROI) becomes a couple of months, not a couple of years, as is typically the case for traditional "Service Assurance" tools.

## Lucent Technologies *Navis*® iOperations Software Solutions

*Navis*® iOperations software is a comprehensive portfolio of multi-vendor, multi-technology Operations Support Systems for wireline, wireless, optical, circuit and data networks. *Navis*® iOperations systems are developed on extensible, programmable platforms, open APIs and advanced system architecture to provide carrier class reliability and scalability, as well as rapid and affordable integration into a Service Provider's preferred operations infrastructure.

The award winning Lucent *Navis*® iOperations portfolio, including VitalSuite® and VitalQIP™ network management software, support the breadth of Network Management Operations, including Service Provisioning, Service Assurance, Element Management, Mediation, and Modeling. *Navis*® iOperations solutions enable the delivery of advanced services across current and next generation networks – while improving efficiencies, significantly reducing operating expenses and delivering the Quality of Service that customers demand.

*Navis*® iOperations Software solutions are supported by Lucent Worldwide Services (LWS), Systems Integrators, and Service Provider partners who provide a comprehensive suite of world-class planning, deployment, operations and maintenance services.

For more information, contact your Lucent Technologies sales representative or call 1-888-426-2252 or visit the Lucent Technologies web site at www.lucent.com.

This document is for planning purposes only, and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to these products or services. The publication of information in this document does not imply freedom from patent or other protective rights of Lucent Technologies or others.

*PricewaterhouseCoopers 2000

*Navis* and VitalSuite are registered trademarks and VitalQIP is a trademark of Lucent Technologies.

Copyright © 2003, Lucent Technologies, Inc. All rights reserved.