BEFORE THE FLORIDA PUBLIC SERVICE COMMISSION

DIRECT TESTIMONY

OF

WILLIAM L. WILEY

DOCKET NO. 041144-TP

Q. Please state your name and business address.

A. My name is William L. Wiley. My business address is 6550 Sprint Parkway, Overland Park, Kansas, 66251.

Q. By whom are you employed and in what capacity?

A. I am employed by Sprint Local Telecommunications Division as a National Engineering Standards Manager IV – C2P. In this proceeding I am testifying on behalf of Sprint-Florida, Incorporated.

Q. Please describe your work experience with Sprint.

A. I began my career with Sprint as a Central Office Equipment (COE) installer, completing 6 years in this field. In 1980, I became a COE Engineer, working on equipment additions to various central offices and switching systems. In 1987 I became a Signaling Systems planning engineer, developing plans for the initial rollout of Signaling System 7 to the Sprint network. In 1990, in addition to SS7 planning I also worked on

switch systems planning, developing features and functionality of Sprint's Long Distance switching network.

From 1992 to 1997, I became one of Sprint's representatives to T1S1, A standards body associated with signaling and switching systems. Also at this time, I was chosen to be one of Sprint's representatives to the International Telecommunications Union. This body establishes standards for telecommunications for the world.

In 1997 I became a part of a team that worked on developing a new form of switch and signaling platform. In my position, I developed call processing and signaling processing for the platform. Because of this work, I became the co-inventor of 44 United States patents.

In 2002, I became a National engineering standards manager for the implementation of C2P, a new type of switching system, for the local telecommunications division of Sprint.

Q. What is the purpose of your testimony in this proceeding?

A. The purpose of my testimony is to provide the facts surrounding the SS7 messaging and parameters derived from the call records obtained from the Agilent system that Sprint uses to determine traffic patterns and abnormalities derived from calls destined for the Sprint LTD network.

Q. Could you please provide an overview of your testimony?

A. Yes. In my testimony, I will outline the facts concerning KMC's transmission of call setup information to Sprint and KMC's passing of charge party, calling party and jurisdiction information parameters that show the passing of interstate and intrastate interLATA traffic over local interconnection trunks to Sprint. I am providing testimony for the following issues in Order No PSC-05-0125-PCO-TP:

Issue 4 What is the appropriate method to determine the jurisdictional nature and compensation of traffic?

Issue 5 Did KMC knowingly deliver interexchange traffic to Sprint over local interconnection trunks in violation of Section 364.16 (3) (a), Florida Statutes? If yes, what is the appropriate compensation and amount, if any, due to Sprint for such traffic?

Issue 8 Did KMC deliver interexchange traffic to Sprint over local interconnection trunks in violation of the terms of the Interconnection Agreements with Sprint? If yes, what is the appropriate amount, if any, due to Sprint for such traffic?

Q. What systems and information were used to determine the accuracy of the call records between Sprint and KMC?

A. The Agilent system is used by Sprint to extract Signaling System 7 Call setup messages and record the information so that traffic patterns and signaling abnormalities can be reviewed and corrected. For this testimony, I will discuss the information captured by this system as it relates to KMC's local interconnection trunk groups interconnected to Sprint and how data collected was used to develop the usage by the appropriate jurisdiction.

Sprint is interconnected to KMC via a local interconnection trunk group that uses signaling system 7 (SS7) for call by call signaling. This Network to-Network interconnection (NNI) system provides "out of band" call detail signaling information that sets up, provides supervision, and disconnects supervision for telephone calls.. Instead of using tones to pass routing and number identification information over the circuits used for the voice path of the call, SS7 sends this information over a separate link and correlates this call setup information with the voice circuit connected between two switches. With this type of signaling, much more call detail information can be passed, providing for more services and better call control for each switching entity.

In SS7, there are approximately 5 messages that are sent between the switching entities that control the establishment, duration, and disconnection of calls between the network elements. The five messages are as follows:

Initial Address Message (IAM) – This message provides call setup instructions from the originating switch to the terminating switch. This message contains information for the routing of the call, information on the originator of the call, charging information, and bearer requirements for the call if applicable. It also provides instructions to the terminating switch concerning which circuit the voice bearer path will be using. This is the primary message that initiates a call between the two switching entities.

Address Complete Message (ACM) – This message is sent from the terminating switch to the originating switch denoting that a voice path has been established and the call can proceed.

Answer Message (ANM) – The ANM provides an indication back to the originating switch that the call has been answered and the conversation can start. It also provides the indication that timing can start for billing purposes.

Release message (REL) - This message, sent in either direction, signifies that one of the parties has disconnected and the call is over. It also provides the end of call indication for billing.

Release Complete Message (RLC) – this message is sent to confirm that the call has been terminated and the circuits associated with the call have

been released.

There may be more messages that are passed between the two switches associated with the call, but for Sprint's analysis, the above mentioned messages are the five used. Most of the information extracted by the Agilent system is derived from the Initial Address Message (IAM).

Q. Please explain in layman's terms the Agilent system, what it does, and the output it produces.

A. In simple terms, the Agilent system looks at call detail records extracted from the SS7 system described above. Using the originating telephone number and the terminating telephone number, Agilent determines if a call is local or interstate or intrastate interLATA. Information about Agilent is attached to my testimony as Exhibit WLW-1.

Q. What information was used to determine that calls were being incorrectly routed by KMC over its Local Interconnection Trunks with Sprint?

A. The Agilent system captures the SS7 messages and their parameters for each terminating call sent over the SS7 network corresponding with the local interconnection trunks from KMC to Sprint. It then takes these messages and related provisioning information to form a report that shows the various details and parameters of the call.

In looking at the reports provided, three basic fields were used to determine routing and the origination information of the calls. These items were Calling Party Number, Charge Number, and Jurisdiction Information Parameter. These parameters determine the originator of the call, the billing number for the call, and the switch entity where the call was originated. The Called party field was also reviewed to ensure the number was local and appropriate to route over the trunk group in question.

To develop a better understanding of these above mentioned parameters, I will provide a description of each parameter and its usage within SS7 from the Local Switching System Generic Requirements, published by Telcordia Technologies, which determines the basic switching requirements of the Public Switched Telephone Network. This document gives the following definitions for the three parameters under discussion.

Calling Party Number (CPN)

The format and coding of the calling party number parameter is similar to that of the called party number parameter.

An originating Stored Program Controlled Switch (SPCS) shall include the CPN in the IAM, when available. When included, the CPN can be used to facilitate features at the terminating end such as calling number display, selective call waiting, selective call forwarding, and selective call rejection.

The calling party number parameter shall include the address digits of the specific station set originating the call.

NOTE: The calling party number need not be the same number provided by the Automatic Number Identification (ANI) feature of the inband exchange access signaling described in GR-690-CORE, *Exchange Access Interconnection, FSD 20-24-0000*. For example, if the station set is behind a Private Branch Exchange (PBX), the number provided by the MF ANI feature might be the main PBX line number rather than the number of the specific station set. The number of the specific station set may be available to the originating SPCS as the calling party number.

The originating end office shall determine whether the restriction of calling party address presentation applies for a particular call based on the class of service associated with the calling subscriber's line.

If the calling party number is restricted, the address presentation restricted indicator, bits DC in the second octet of the calling party number, shall be coded 01, "presentation restricted." Otherwise, these bits shall be coded 00, "presentation allowed."

Charge Number (CN)

The Charge Number (CN) parameter is of variable length.

An originating SPCS shall be able to include or to not include the CN, as a pair with the Originating Line Information Parameter (OLIP), in an IAM based on the outgoing trunk group and class of service (i.e., originating screening and routing options).

In addition, the CN shall be omitted from the IAM at the originating SPCS if all of the following conditions are met:

• The OLIP and the CN are to be provided on the outgoing trunk group.

• The CPN parameter is included in the IAM.

• The CN address digits agree with the CPN address digits.

... The presence of the OLIP together with the absence of the CN parameter will inform the receiving SPCS that the CN address agrees with the CPN address.

The CN parameter shall provide the ANI for the call and the ANI shall be available and identifiable for each call, at each SS7 originating SPCS, and at each SS7 intermediate SPCS serving as an originating SPCS.

When included, coding of the Charge Number parameter shall be as follows:

... When included, the CN parameter shall contain, when available, the ten NPA+NXX+XXXX address digits of the ANI in the address information field of the parameter.

... If ten address digits are available in the address information field, the odd/even indicator bit shall be coded "even number of address digits," and the nature of address field shall be coded "ANI of the calling party; national number."

... If the ten address digits are not available, but the Numbering Plan Area (NPA) digits are available, then only the three NPA digits shall be sent in the address information field.

... If only the three NPA digits are available in the address information field, the odd/even indicator bit shall be coded "odd number of address digits," and again, the nature of address field shall be coded "ANI of the calling party; national number."

... The numbering plan field shall be coded "ISDN numbering plan (ITU-T Rec. E.164)" when either three or ten digits are sent.

... If no ANI address digits are available, the odd/even bit shall be coded as "even number of address digits," and the nature of address field shall be coded "ANI not available or not provided."

... In the case when no ANI digits are available, the octet containing the nature of address code shall be the last octet of the CN parameter.

Jurisdiction Information Parameter (JIP)

An originating SPCS shall be able to include or not include the JIP in the IAM as a LEC option based on the outgoing trunk group.

Although the inclusion of the JIP in the IAM is a LEC option, with the introduction of LNP, it is expected that the JIP will be included in the IAM for all calls. The JIP is used in LNP to signal the first six digits of the Location Routing number of the switch serving the calling party. The use of the JIP in LNP is further described in GR-2936-CORE, *Local Number Portability (LNP) Capability Specification: Service Provider Portability*

In normal operation, the calling party number and charge number could be

used in the same IAM if the CPN and CN were different. But unlike the calling records of the calls from KMC, the CPN and CN should have a relationship between the two. As with stations behind a PBX, the station numbers would be populated in the Calling Party Number while the Charge Number parameter would be populated with the billing number of the PBX itself.

The charge number is a provisionable field that denotes the billing number of the trunk group it supports. This field is assigned by the carrier at the originating switch. This type of provisioning is usually confined to User – Network trunk groups. That is, trunk groups that interconnect the carriers switch to a user's PBX or customer premise equipment. Signaling for these trunk groups could employ Dual Tone Multifrequency (DTMF), Multifrequency (MF) or Integrated Services Digital Network (ISDN) signaling as in a Primary Rate Interface.

The Jurisdiction Information Parameter denotes the Jurisdiction of the originator of the call. That is the location of the switch where the call originated. It is used in Local Number Portability to denote the originating NPA.NXX of the call.

Q. What did the SS7 information related to the calls Sprint received from KMC reveal in relation to the Telecordia standards described above?

A. With Sprint's research, the Agilent system provided information which

With Sprint's research, the Agilent system provided information which showed that a large percentage of calls coming from KMC's switches did not meet the standardized criteria for CN, CPN and JIP. The records showed that while the charge number and JIP were attributed to the KMC switch and the calls purportedly originated within KMC's network switches, the calling party number revealed that the calls actually originated in areas outside of KMC's network. A large percentage of these calls were Intrastate InterLATA calls. This information indicated that KMC had violated its agreement with Sprint concerning the proper Local Interconnection trunk arrangements as explained in Mr. Burt's testimony.

This population of originating calling party numbers outside of the local access area over originating PRI trunks was not relegated to a small number of trunk groups. Through Sprint's research from traffic collected on the Sprint-KMC local interconnection trunks, approximately [redacted] trunk groups ([redacted] in Tallahassee and [redacted] in Fort Myers) that had an originating Charge number and JIP assigned to the KMC Switches were found to carry traffic that originated outside the serving area. These calls could not have come from other switching entities and tandemed through the KMC switch. Since the JIP and CN both are assigned to KMC, the trunk group(s) would have to originate the traffic unless non standard routing or digit manipulation occurred.

Q How did Sprint determine the appropriate jurisdiction of the traffic that KMC was passing to Sprint over the local interconnection trunks?

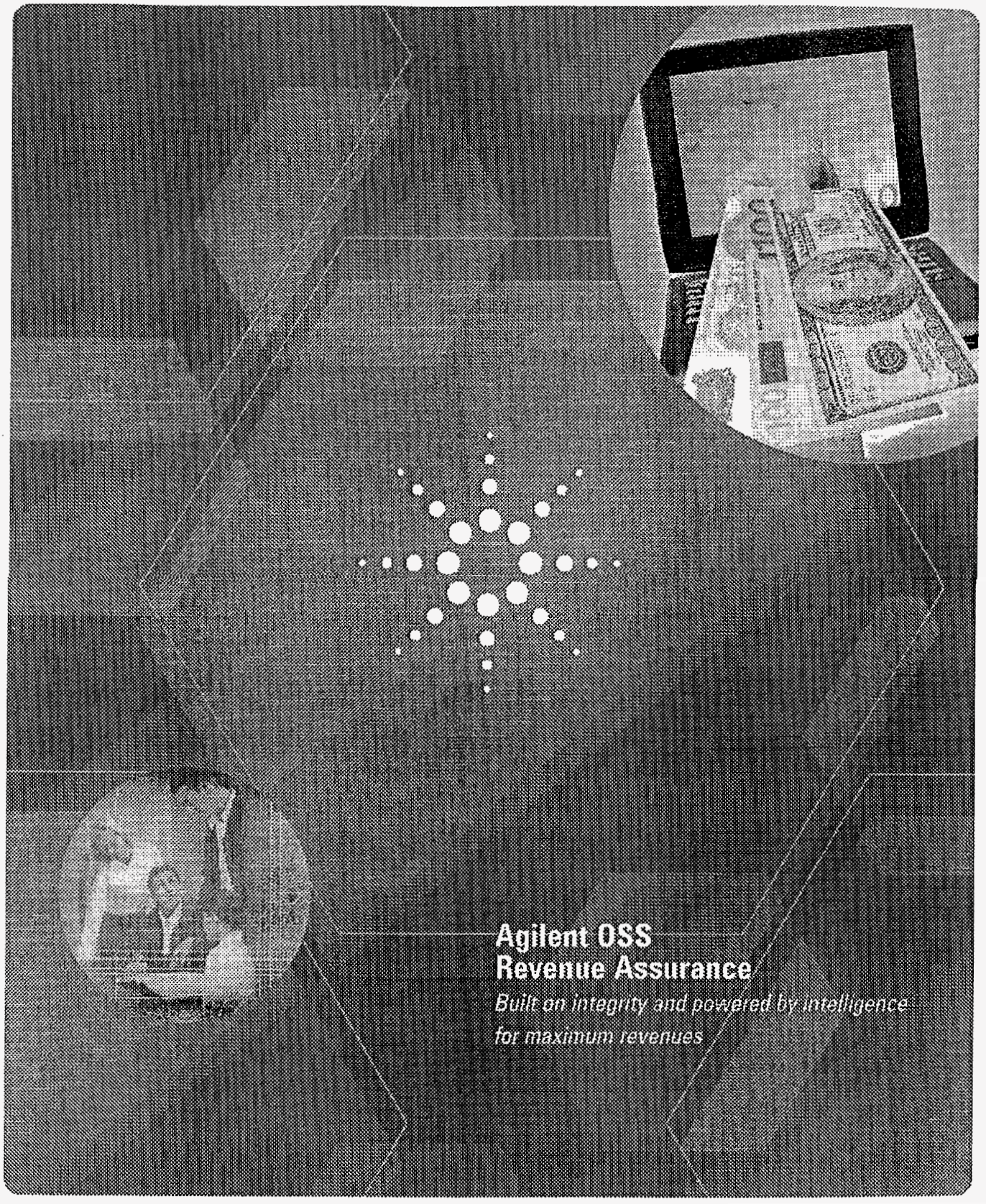
A. Sprint used SS7 records and Agilent, as described above, to identify the proper jurisdiction of the traffic. The jurisdiction was based on the calling party numbers to the called party numbers in the SS7 call detail records. To determine the amount of access charges KMC would have been billed had the traffic been routed properly, Sprint developed a percentage of interstate, intrastate interLATA and local traffic based on the Agilent study. These percentages were applied to the MOUs from June of 2002 through November 2004 to develop the access charge billing amounts KMC should have been compensating Sprint. These calculations are discussed in more detail in Mr. Farnan's direct testimony. These same records were used to determine that the amount of traffic for which KMC received compensation at the local voice rate was more than it should have been. These calculations are discussed in more detail in Mr. Danforth's direct testimony. Attached to my testimony as Exhibit WLW-2, is the Agilent study that was used to calculate the access and local minutes.

Q. Can Sprint produce call detail records to support its findings concerning KMC's delivery of interexchange traffic to Sprint over local interconnection trunks with a local number?

A. Yes. Attached to my testimony as Exhibit WLW-3, are the call detail records supporting the Agilent study. While, theoretically, Sprint could produce all of the call detail records associated with the traffic that is the subject of this dispute, it is unnecessary and would be unduly burdensome and expensive for Sprint to do so. Sprint maintains only six months of the call detail records online (although they include partial months back to January 2004). The remaining data is archived on tapes with a third party vendor. It takes approximately two days to pull and process a calendar day of call detail records from archives. Instead, Sprint has developed a statistically valid random sample of the call detail records, as described in the affidavit from Sprint's economist Dr. Brian Staihr and attached to my testimony as Exhibit WLW-4, to support its allegations. Records reflecting 11 days of the 27 days included in the random sample are attached to my testimony as Exhibit WLW-5. Because of the length of time required to pull and process each calendar day of records, Sprint is still compiling the records for the remaining 16 calendar days included in the random sample. Sprint intends to file a Revised Exhibit WLW-5 as soon as the additional data is available.

Q. Does this conclude your testimony?

A. Yes, it does.



Agilent OSS Revenue Assurance

Built on integrity and powered by intelligence for maximum revenues

Agilent Technologies

Punctured profits - how revenues can drain away

Agilent's OSS Revenue Assurance portfolio of flexible, integrated solutions helps telcos significantly reduce costs and revenue leakages. The solutions are based on solid network data, which provides the irrefutable facts needed to support a wide range of business functions - billing audit, traffic planning, fraud and arbitrage detection and interconnection analysis. Their deployment has already saved Agilent customers hundreds of millions of dollars.

Revenue loss presents a major challenge to the telecommunications industry. With estimates of annual revenue leakage ranging from 3% to 11% of gross revenues, the scope of the problem and finding the means to combat it have now assumed critical importance.

Increasingly complex network architectures, the demands posed by multiple data sources, and the inter-organizational stress resulting from mergers and acquisitions all create hundreds of opportunities for revenue leakage.

Operators have identified the main causes of leakage as: poor processes and systems; difficulty with systems integration and synchronization; interconnect errors; incomplete or incorrect Call Detail Records (CDRs) and credit management. Other causes include fraud, billing system errors, and errors relating to the introduction and pricing of new products and services. In nearly every case, losses can be attributed to bad data generated by network elements or business processes - records that are missing, incomplete or totally wrong.

The economic pressure to reduce costs and sweat assets has pushed Revenue Assurance (RA) to the top of the business agenda. Telcos need to ensure they collect the revenues due for the services they provide. Plugging revenue leakages - quickly and permanently - represents pure profit.

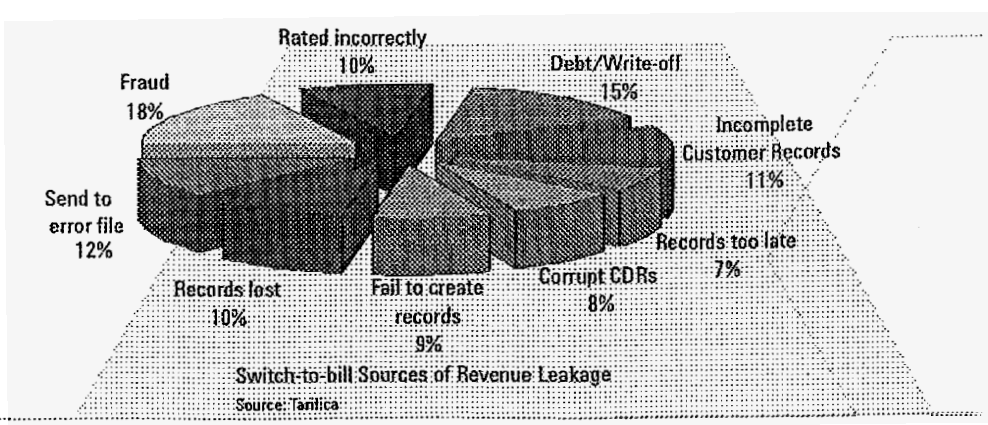
Revenue Assurance is usually regarded as a business problem, to be addressed by staff with specialist financial or business skills. Yet this approach may not go deep enough to identify the true causes of the problem. If billing records from network elements - the primary data input to a billing system - are missing, faulty or in error, no amount of clever processing can ever produce the correct results.

Input data quality has a direct bearing on ultimate business failure or success.

Agilent approaches Revenue Assurance from the network perspective, basing its portfolio of RA solutions on data extracted from the network. The data is independent of the network elements and provides a gold-standard reference of every individual call and service transaction. This network-centric view offers a unique set of business-critical insights and helps an operator realize the true worth of all its activities.

But Agilent is able to offer much more than just a reliable, accurate source of network data. Its extensive portfolio of RA solutions and services demonstrates a deep understanding of business processes and requirements and wide-ranging analytic capabilities. Strategic partnerships with industry leaders focus on achieving financial benefits, including accurate billing, audit and reconciliation, and combating fraud. In short, Agilent enables enterprise-wide returns.

Agilent has the precision, power and performance to maximize revenues and the potential for profit - where it matters most.



Realizing the value of network data

Agilent's network monitoring and management systems are recognized throughout the world as the market leaders. They collect and analyze information from wireless and wireline networks supporting multiple technologies including SS7, VoIP, 2G, 2.5G and 3G. Totally independent of network elements, they provide impartial views of what is happening on a network even during fault conditions.

A broad suite of applications provides invaluable insights for the network operations and engineering teams responsible for Network and Service Assurance and the business teams responsible for Customer and Revenue Assurance.

Agilent's monitoring systems offer operator-class performance and scalability with call volumes exceeding half a billion records per day, and multi-terabyte data warehousing capability.

As a long-standing leader in Revenue Assurance and Business Intelligence, Agilent has exploited this valuable data resource to the full. Agilent solutions are instrumental in generating millions of dollars of additional revenue for telcos around the world. Virtually all Tier 1 US Regional Bell Operating Companies (RBOC) and Incumbent Local Exchange Carriers (ILEC) use them for wholesale/interconnect billing and billing verification and they are regularly deployed to support US FCC filings, court cases and interconnect disputes.

Agilent takes a network-centric approach to Revenue Assurance to provide a single version of the truth. It is a critical data source to ensure billing occurs for chargeable network events. Agilent's Revenue Assurance portfolio represents the most valid option for telcos who are seriously looking to address cost and revenue leakage on an enterprise-wide basis.

Comprehensive	*Accurate*	*Efficient*
Correlates all legs of complex calls (AIN, 800, VoIP, etc) and captures more parameters than standard switch records.	Precisely timed, complete records of service usage.	Imposes no load on network elements.
Visibility of calls where switches have not generated records (incoming test calls).	Provides real-time in-progress call data.	Consistent output format - no need for complex mediation.
Shows abnormal call or transaction events (incomplete, unanswered).	Data available immediately for real-time applications, or via reliable batch transfers for off-line analysis.	Probes can be targeted to collect specific data feeds - roamers, IN, Mobile Location, RF QoS, Interconnect, Core network, Access network, IP backbone, etc.
One system combines circuit-switched signaling with packet-switched control and service usage data.	Proven hardware architecture captures all traffic - even during network overloads.	Scalable - systems can range from focused coverage of a few gateway links, to full coverage of an entire network.

Powerful solutions to maximize revenues

Agilent's Revenue Assurance portfolio plays a key role in helping telcos increase the profitability of every aspect of their operations and extract the maximum revenue potential from all technologies and services. The solutions provide the accurate, timely analysis of multiple data feeds - including SS7 CDRs, VoIP records and wireless transaction records - to support business decisions in three main target areas:

Interconnect and Wholesale Management

Interconnect and wholesale traffic represents the biggest single item on every telco's balance sheet. Ensuring accurate interconnect bills and impeccable interconnect quality can have a major impact on overall profit. Agilent provides several Revenue Assurance solutions in this area.

Routing international calls to balance cost is a complex business requiring real-time performance data to manage interconnect routing dynamically, taking advantage of competitive spot rates, without compromising quality. Agilent provides the real-time performance management tools to optimize the blend. But rapidly changing interconnect relationships are a headache for the wholesale billing department, who must ensure that bills are accurate, otherwise the benefits of dynamic re-routing are lost. Agilent provides accurate records of interconnect traffic to generate and verify interconnect bills.

The ever-growing demand for innovative telecoms services has dramatically increased the volume and complexity of signaling traffic. Interconnect carriers who process this traffic need detailed information on signaling network usage to plan network capacity and generate accurate bills. Here again, Agilent provides the solution.

The Network-to-Bill Revenue Integrity

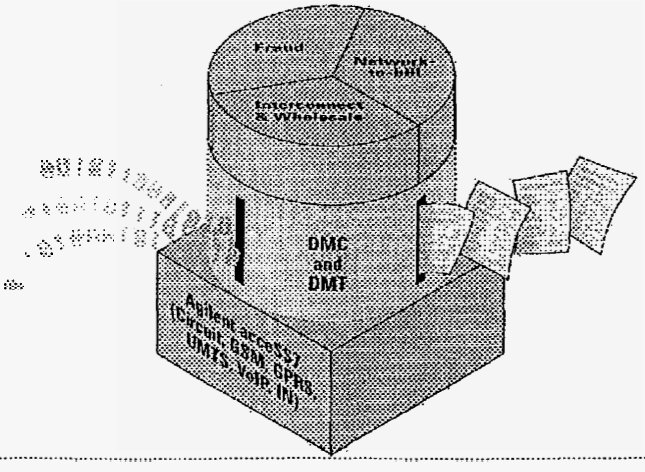
Turning network CDRs into customer bills is a complex, dynamic, multi-step process. CDRs come from hundreds of diverse network elements. They must be gathered from network-wide collection sites and mediated into a common format. Each CDR is then rated, based on a combination of parameters which include time, duration, distance, location and type of service; rating tables often contain hundreds of thousands of entries. Rated CDRs are then aggregated into individual customer bundles and discounted to reflect types of customer and service packages. Finally, recurring charges are applied to generate the customer invoice. Change occurs with every billing cycle: new switches, services, tariffs, features, customers, and system upgrades and expansions. Merely keeping the system running is a full-time task, and inevitably errors and leaks accumulate.

Agilent's in-house and best-in-class partner solutions span this entire network-to-bill chain, verifying translations, analyzing errors and dropped log files, reconciling records, identifying and correcting the root cause of problems, auditing each stage and ultimately recovering revenues. The end result is a continuous process improvement and a permanent fix of revenue leaks.

Retail and Wholesale Fraud Management

Communications networks throughout the world have always been vulnerable to opportunistic and organized fraud. It is one of the most significant areas of revenue loss, estimated to cost the global telecommunications market some $50 billion each year. As new technologies and services come on line, the prevalence of fraud increases. Widespread use of the Internet means that any weakness will be attacked from around the world. Deregulation and competition have also increased the risk of fraud, with business pressures working against strict credit control and detailed customer checks.

Agilent helps to halt this escalating cycle of crime by giving fraud investigators the information they need to take immediate action. All types of fraudulent activities can be flagged as soon as they occur, including subscription fraud, fraud involving other operators such as retailers and resellers and internal fraud. 'Dark' arbitrage can be detected and measured as well as other types of activity such as SMSC bypass fraud and answer-no-charge switch fraud. Profiling and assessing new subscribers and monitoring new sources and products anticipate and prevent fraudulent activity before it is able to do any damage.



Agilent OSS Revenue Assurance solutions portfolio

Agilent's portfolio of Revenue Assurance solutions helps to safeguard the value of a network and its services, maximizes revenues and reduces the cost of operations.

Dedicated Revenue Assurance solutions address specific challenges in these business areas: Interconnect and Wholesale; Network-to-bill; Fraud. In addition, Agilent provides generic data-warehousing and data-mining solutions that enable all departments to explore one-off problems, identify emerging trends and tackle new issues.

Interconnect Analysis

The Interconnect Analysis (IA) solution helps to realize the true value of interconnect traffic, by measuring, recording and jurisdictionalizing inter-carrier traffic quickly and cost-effectively. An expanding portfolio of Interconnect Analysis modules provides the details needed to help assign responsibility, validate charges and negotiate accurate, more profitable interconnect agreements. The modules target specific interconnect challenges, such as:

- o Identifying the jurisdiction of transit traffic
- o Accounting for unbundled, resold and ported lines
- o Identifying inter-carrier toll-free traffic
- o Measuring and jurisdictionalizing wireless traffic
- o Determining the true origin of a wireless call
- o Managing records for long-duration calls
- o Analyzing traffic at trunk group level
- o Combating 'dark' arbitrage
- o Protecting value-added service revenues.

Network-to-bill Verification

Agilent has teamed up with best-in-class partners to offer a broader overall portfolio of Revenue Assurance solutions.

Partner network-to-bill verification platforms provide the basis for a suite of applications and services that automates the Revenue Assurance process and is complementary to Agilent's signaling solutions and data feeds.

The addition of network-to-bill partner solutions to the Agilent portfolio extends the company's solution coverage into the traditional Revenue Assurance domain - the billing chain - to tackle challenges such as:

- o Auditing usage processing at each control point
- o Verifying the presence and accuracy of network transactions from network usage to switch record
- o Carrying out a detailed analysis of error and drop files for recoverable and billable events
- o Validating the accuracy of billing rates for recurring or fixed features across multiple services
- o Demonstrating Sarbanes-Oxley compliance by auditing key revenue systems and processes
- o Providing company-wide visibility and a common platform for Revenue Assurance executive dashboards tracking revenue management.

Automatic Message Accounting Transmitter 7 and Signaling Meter

Automatic Message Accounting Transmitter 7 (AMAT7, US) and Signaling Meter (International), measures SS7 traffic volume to give a totally accurate picture of signaling network usage and resource consumption.

Precise inter-network usage measurements provide wholesale operators with the flexibility to invoice for previously untracked SMS and roaming signaling traffic that transits their networks.

Competitive Access Detail Recording for SS7

Competitive Access Detail Recording for SS7 (CDR7) generates real-time trunk usage measurements that enable telcos to track and bill for interconnect usage. Records are created for every call monitored so that detailed invoices for network usage can be created accurately and easily. CDR7 enables:

- o Correct dimensioning of the transmission network
- o Full payment for resource consumption
- o Verification of interconnect charges
- o Access to key marketing information
- o Instant delivery of more accurate billing data.

Traffic QoS Manager

This high-performance solution provides detailed real-time and historical information on all aspects of interconnect network activity. It provides automatic alarming, flexible analysis and intelligent measurement handling. This enables it to:

- o Monitor and verify inbound and outbound quality of service
- o Determine cost-effective interconnect partnerships
- o Facilitate service level agreement negotiations.

It can also be used for intra-network monitoring, to manage the quality of key services, or to analyze the service delivered to corporate customers and VIPs.

Agilent's enterprise-wide Revenue Assurance solutions open up the rich potential of network data to everyone across an organization.

Cerebrus[RE]

Cerebrus[RE] is a state-of-the-art fraud detection system that focuses on the overall behavior of suspected fraudsters. The solution uniquely combines advanced artificial intelligence applications that use neural networks, with rule and database technologies, providing consolidated, case-oriented, fraud management capabilities.

Cerebrus[RE] provides a platform that can be tailored to the needs of any size of operator. It combines a set of common capabilities with feature packages appropriate for specific markets, technologies and types of operator. For example, the subscriptor package provides pre-activation screening of potential subscribers, helping to minimize the fraud risk while expanding the customer base.

Cerebrus[RE] accepts call records from a wide range of sources, such as billing CDRs, SS7 monitoring systems, roaming record exchanges, 2.5G/3G charging gateways and IP network billing functions and mediation devices. It provides operators with comprehensive network visibility, helping them to detect fraud as it happens and take immediate action to prevent or reduce fraud losses.

Business Support Tools

The Data Management Component and Data Mining Toolkit are integrated products that support decision-making across a wide range of business disciplines.

Data Management Component

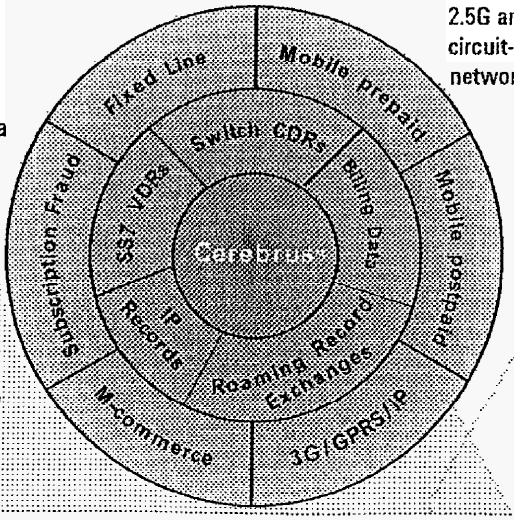
Data Management Component (DMC) handles the storage and management of CDRs and other transaction detail records derived from network monitoring. It is a robust and scalable multi-terabyte data warehouse solution.

Data Mining Toolkit

Data Mining Toolkit (DMT) is an analytic layer that resides on top of the DMC. The Data Mining Toolkit enables users to explore the DMC's data using sophisticated dimensional analysis techniques.

Out-of-the box modules based on best industry practice help to examine a particular service or network technology more closely. They include all the relevant pre-packaged data enrichment, analysis views and measures.

The Data Mining Toolkit streamlines the process of data browsing and extraction, enabling network specialists, planners and decision makers to identify, explore and extract valuable information from a variety of data sources.



They can configure this information in any way they choose and display and share the results with colleagues using a performance portal or DMT dashboard on the web.

Examples of the DMT used for revenue assurance include:

- Loss of revenues through SMS misuse - analyzing international traffic to identify unsecured SMSC, which provide free access, and spotting SMS spam generators which damage customer confidence and absorb network resources
- Interconnect signaling billing - monitoring interconnect SS7 links to analyze traffic trends, predict future usage and bill according to volume and type of transit message
- Capturing inbound roamers - analyzing CDRs from the access network around national entry points - airports, railway stations, etc. This enables wireless operators to determine where drop-offs occur. They can then fine-tune RF coverage to improve the capture and retention of inbound roamers
- Reality-TV-Show SMS voting - validating SMS transactions and checking network performance to ensure that voting is accurate.

Agilent's Revenue Assurance solutions extract the full value from the comprehensive SS7, VoIP, 2G, 2.5G and 3G data gathered across circuit-switched and packet-switched networks.

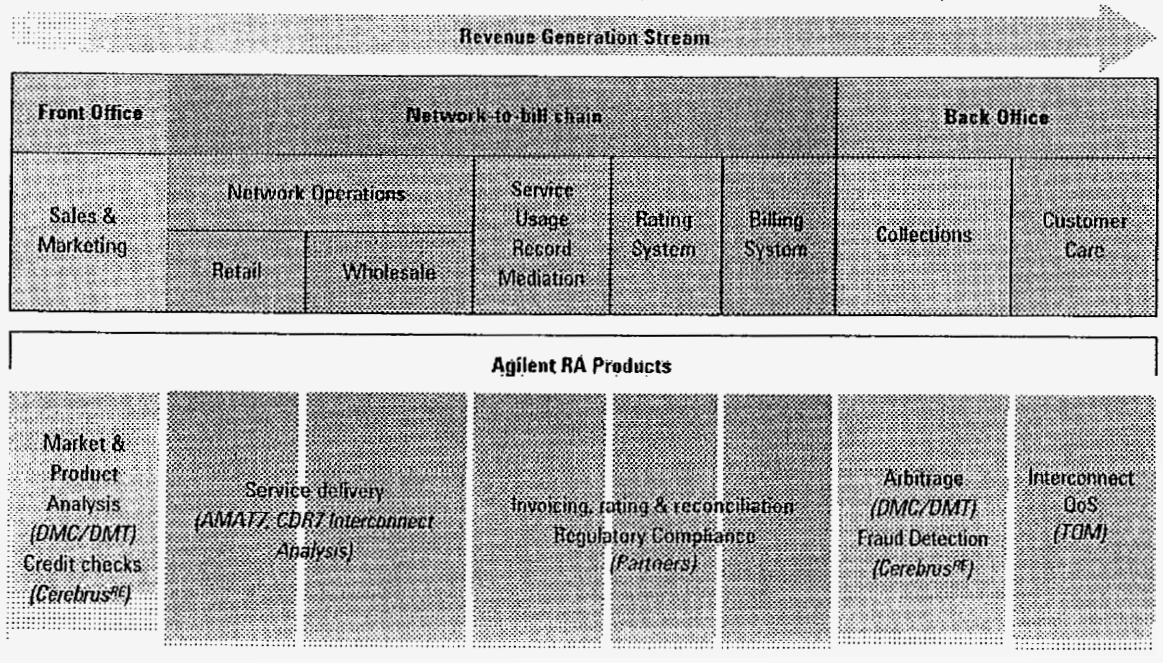
Supporting all stages of the revenue generation stream

Early revenue assurance initiatives took a reactive and labor-intensive approach to revenue loss, tackling each stage of the problem in isolation. The emphasis has now shifted to enterprise-wide deployment, using proactive solutions to address revenue leakage based on end-to-end visibility. The benefits of this approach are substantial - improved productivity, greater customer satisfaction, cost savings and increased revenues.

Agilent's Revenue Assurance portfolio enables telcos to audit and manage every aspect of their revenue generation stream, from initial marketing proposals to final collections. Agilent's deep understanding of business processes and commitment to its customers helps it to deliver focused, relevant solutions, giving every department within an organization the power to maximize its contribution.

End-to-end revenue integrity begins with an independent source of information. When performing revenue assurance analysis on telephony usage, this independent information source is the SS7 record. Increasingly, we see Revenue Assurance departments recognizing the SS7 record independence and using SS7 as a core component of their usage accuracy analysis.

The Yankee Group



Agilent acceSS7 monitoring platform, is absolutely pivotal to the Interconnect Revenue Assurance programs of the large US carriers. The sums of money that Agilent's platform is saving those telcos are very large indeed.

Technology Research Institute

Market and Product Analysis (DMC/DMT)
Analyzing call activity identifies trends and patterns and determines which customers are using, or not using, a particular service. This information is essential for targeting customers, marketing new products and services more effectively, inspiring customer loyalty and generating more revenue.

Credit checks (Cerebrus RE)
Cerebrus[RE] helps telcos to focus attention on high-risk areas and prevent potential revenue losses by profiling new customers and carrying out a series of accreditation checks across all voice, data and m-commerce services before accepting subscriptions.

Service delivery (AMAT7, CDR7, Interconnect Analysis)
Agilent solutions put users in complete control of all aspects of inter-operator activity on their networks. They help to determine the correct jurisdiction for every originating, terminating or transit call so that all fees charged and payments made reflect the true situation.

Invoicing, Rating and Reconciliation
Best-in-class partnership solutions perform comprehensive analysis of the entire billing process by auditing and reconciling network-generated CDRs and comparing those to the outputs of mediation, rating and billing systems to ensure all usage-based charges are accurate, complete and timely. It offers the fastest and most efficient path to revenue recovery, cost reduction and customer satisfaction.

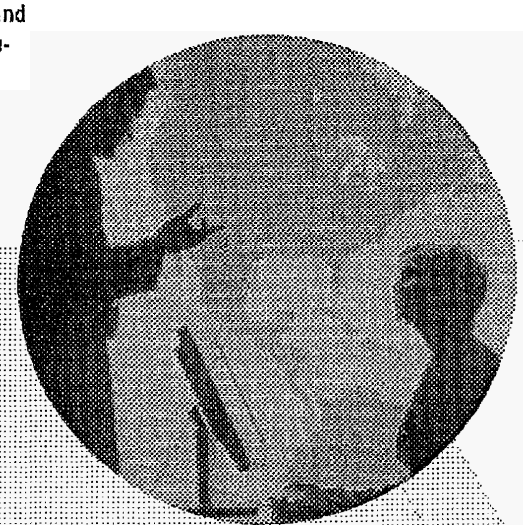
Regulatory Compliance
Partner Solutions provide a robust framework to support compliance with regulatory requirements. In the case of Sarbanes-Oxley, it is able to ensure the accuracy of in-house systems and data, analyzing the data and presenting meaningful results in real time. Requirements such as Real-Time Disclosures, CEO/CFO Certification of financial reporting and Management Assessment of Internal Control are all fully supported.

Arbitrage (DMC/DMT)
The complexity of interconnections between telcos can lead to inadvertent mis-routing of traffic. This may cause network congestion, poor service quality and erroneous interconnect charges. The darker side of this picture is when unscrupulous operators deliberately mis-route and disguise traffic to take advantage of differentials in interconnect-rates. The solution to these problems is to analyze SS7-based CDRs, which reveal the actual routes taken by interconnect traffic, and the true origin, destination, and class of each call.

Agilent has developed a set of analysis tools and templates which run on the DMC data warehouse to simplify the detection of arbitrage. Telcos who use these solutions have recovered millions of dollars of lost revenue, and have conducted successful prosecutions against persistent offenders.

Fraud Detection (Cerebrus[RE])
Cerebrus[RE] is the most robust and reliable telecoms fraud solution currently on the market; capable of providing an operator with up to 95 percent visibility of fraud within their network. It provides rapid response to new variants of fraud and its accuracy significantly reduces the loss from most types of fraudulent behavior.

Service Quality (TQM)
Service providers are more dependent than ever on the quality and reliability of other operators' networks and services. Agilent TQM is able to deliver fast accurate reports and detailed analyses of network traffic to help telcos manage the quality of service delivered to them by other operators. This results in increased revenues and greater customer satisfaction.



Agilent Solutions meeting Revenue Assurance challenges

Arbitrage detection

Problem	Other carriers exploiting rate differentials for various traffic types by disguising one type of traffic as another.
Solution	Using the SS7 CDRs in Agilent Interconnect Analysis application, the Local Exchange Carrier (LEC) was able to demonstrate that calls were being tampered with in order to disguise their true nature, e.g. by changing Calling Party Number (CPN).
Result	Successful prosecution, with over $20 million paid back to LEC.

Validation rate plan

Problem	A European incumbent wireline operator suspected that it was not recovering all the revenues it was due.
Solution	Network-to-bill wireline postpaid usage assurance solution carried out a SS7-AMA reconciliation. This found that some trunk groups and Incumbent Exchange Carriers (IXCs) were not recording CDRs and no bills were generated.
Result	A large number of errors in non-billable files were identified, representing a significant annual revenue recovery opportunity.

Multimedia HACK, SCAM & SPAM

Problem	Malicious use of multimedia services: o SPAM (inappropriate content) was causing churn o Web SCAMs (e.g. phoney Websites targeting credit card capture) o Weaknesses in TCP/IP stack - handsets were at risk.
Solution	Agilent DMT, was used to track web-site usage categorised by content type, using IP data records enriched with subscriber ID, and alerted on unusual usage: o TopN SPAM IP detail records o Hotlist 'SCAM' websites and identify affected users o IPDRs on certain unsafe ports (mobile viruses) o Identified inappropriate content providers.
Result	SPAM was reduced, hacking intercepted, and SCAMs shut-down with minimal customer impact.

Interconnect traffic performance & QoS management

Problem	Long-haul traffic (e.g. international) was frequently routed via 3rd parties on the basis of cost, with no consideration of effectiveness.
Solution	Using Agilent Traffic QoS Manager, operators measured the actual Call Completion Rate achieved by each of their partners and have renegotiated agreements and re-routed traffic to take account of both cost and completions.
Result	Increased profits.

Billing for SMS & roaming service

Problem	Short Message Service (SMS) and roaming services have increased traffic on a large European operators' network gateways more than 70 percent, fueling costly network capacity expansion.
Solution	Agilent acceSS7 Signaling Meter provided the operator with an alternative to increasing tariffs to fund network expansion by enabling them to accurately bill for each interconnect partner's actual network consumption.
Result	The operator created a new revenue stream that covered the cost of network growth necessary to meet its interconnect partners' service needs. The operator can now charge individual interconnect partners for only the signaling usage that they use.

SMS routing abuse

Problem	Subscribers discover they could route inter-operator SMS messages via the SMSC of a 3rd-party network, thus bypassing operator's SMSC and billing system.
Solution	Using SS7 Transaction Detail Records (TDRs) in Agilent DMT, operator was alerted to the existence of the problem. Analysis of the TDRs identified the SMSC in use. The network was then reconfigured to close off this route.
Result	Daily savings of $75,000.

Addressing multi-way call fraud

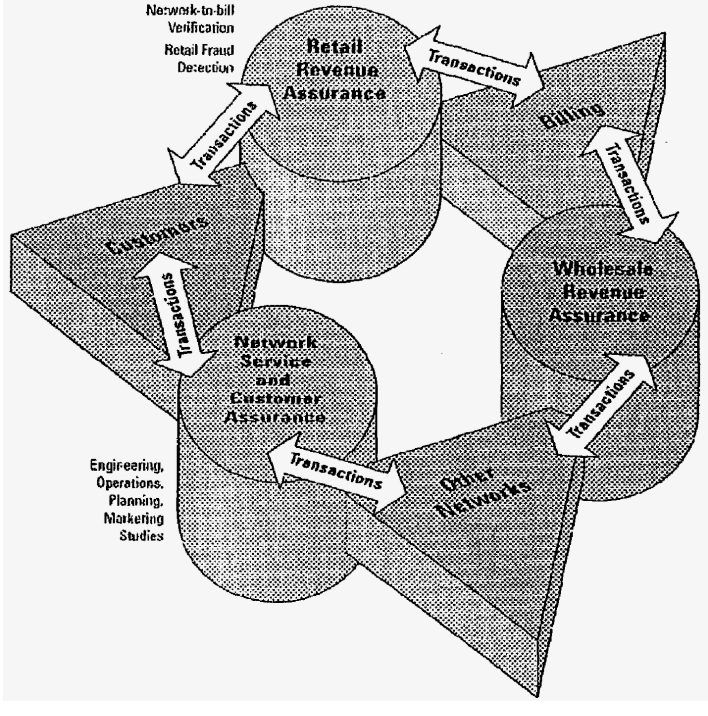
Problem	Equipment misconfiguration permitted calls to toll-free numbers when put on hold to permit calls to a second number. This was abused with international calls and calls to Premium Rate Services.
Solution	Cerebrus[RE] generated alarms for overlapping calls and excessive use of conference call feature by pre-paid customers with no access to these features.
Result	The operator was able to solve the problem before it became more widely known and exploited by its pre-paid base. Estimated savings were $2 million.

Agilent OSS Revenue Assurance

Agilent's acceSS7 monitoring systems play a key role in Revenue, Network, Service and Customer Assurance. They gather, store and process data from multiple technologies, including SS7, VoIP, 2G, 2.5G and 3G, providing detailed information about the status of all transactions across entire networks in real-time. This network-centric view benefits the whole organization. It provides valuable insights into the way systems and customers interact and opens up new ways to safeguard and increase revenues.

The acceSS7 platform supports an integrated range of Revenue Assurance applications targeted at the network-to-bill, interconnect and wholesale and fraud areas. The system's ability to capture **every** network transaction helps to verify the accuracy of wholesale and retail transactions, identify service abuse and fraud, and manage interconnect services and billing more efficiently. Decision makers in all business sectors can also develop new network and marketing strategies, extracting valuable information from this gold standard of reference data and sharing these insights **across** the organization.

Agilent's OSS Revenue Assurance solutions provide you with quickly deployed capability to increase revenues, manage your network more efficiently and meet customer expectations.



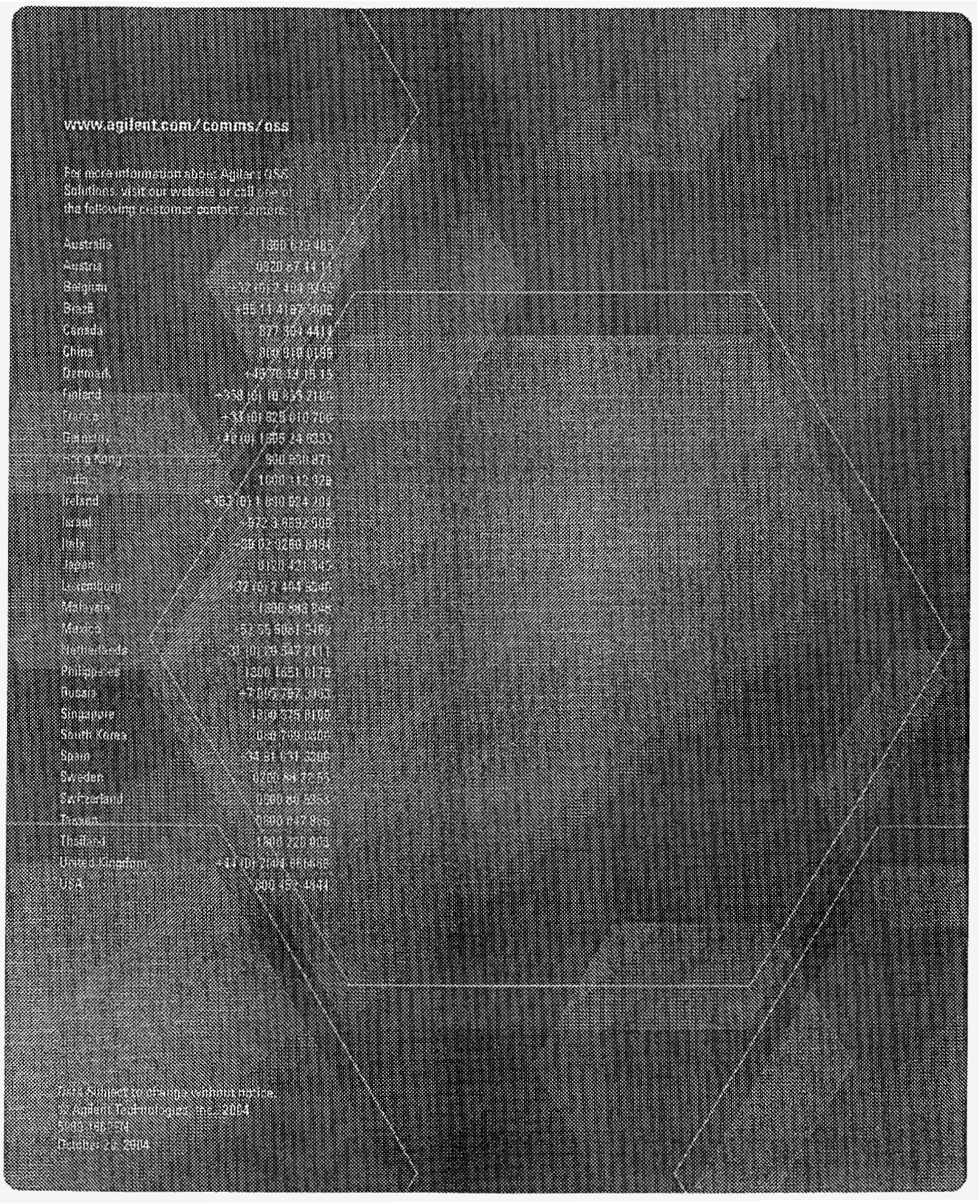
Agilent Professional Services

A full range of consultancy, integration and tailored support services complement the acceSS7 Revenue Assurance portfolio. Solution Consultants will work with you to define your business and technical requirements in detail and develop a precisely targeted solution. Agilent's extensive experience in delivering complex systems ensures a smooth installation and commissioning process, with expert system integrators embedding the solution within your own OSS environment. This minimizes on-going system management costs.

Training classes, implementation and value-added consulting services make sure that your staff can use the solution to maximize your investment. Agilent's worldwide support organization provides the breadth of services to let you select the package of proactive and reactive support that exactly meets your needs.

About Agilent

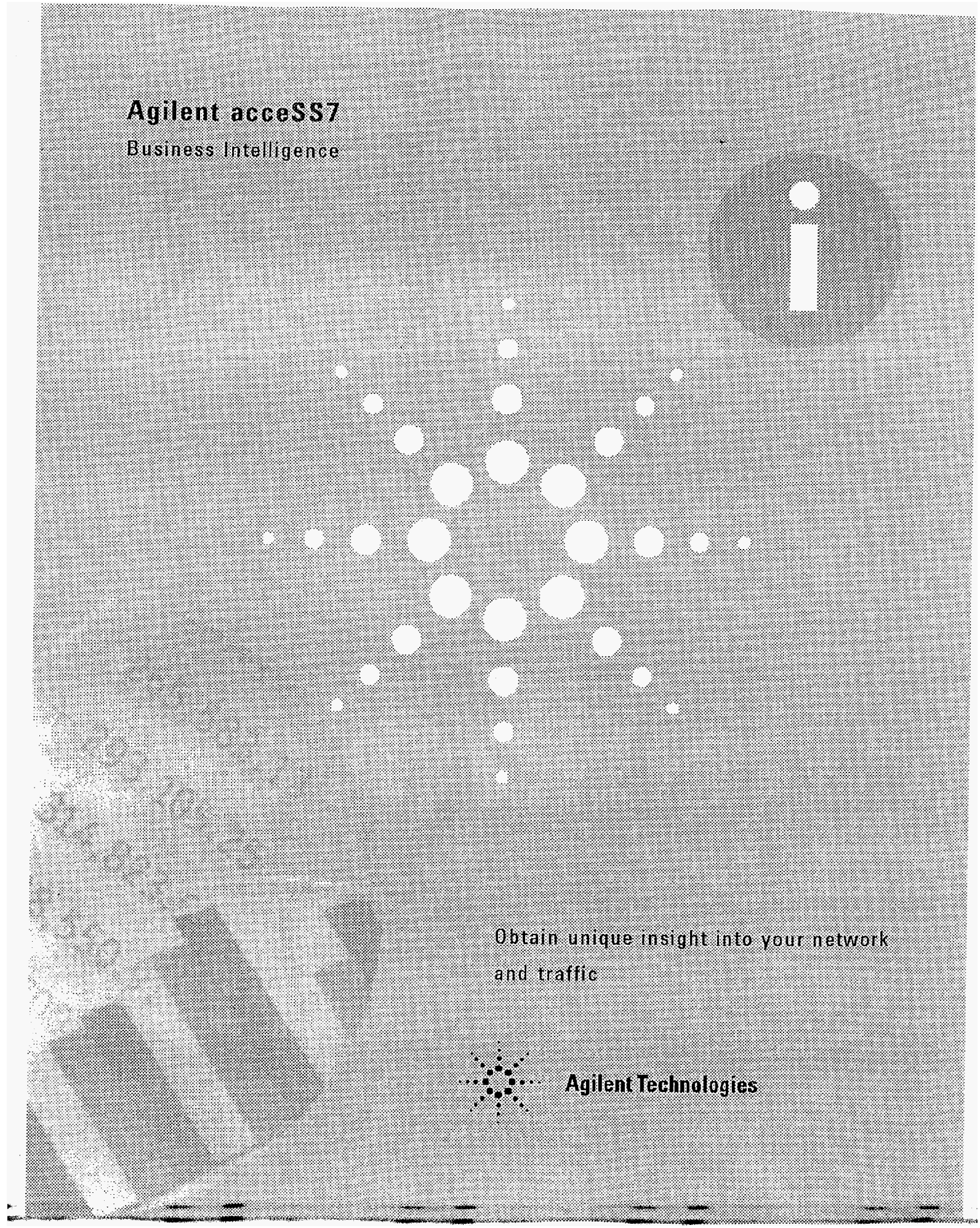
Agilent Technologies is a leading provider of components, test, measurement, monitoring and management solutions for the communications industry. Agilent enables designers, manufacturers and service providers to accelerate the delivery of next-generation devices, networks and services. Its broad set of solutions and services include optical, wireless, Internet and broadband technologies that span the entire revenue generation stream. Agilent's 28,000 employees serve customers in more than 110 countries. Information about Agilent is available on the web at www.agilent.com



Agilent Technologies

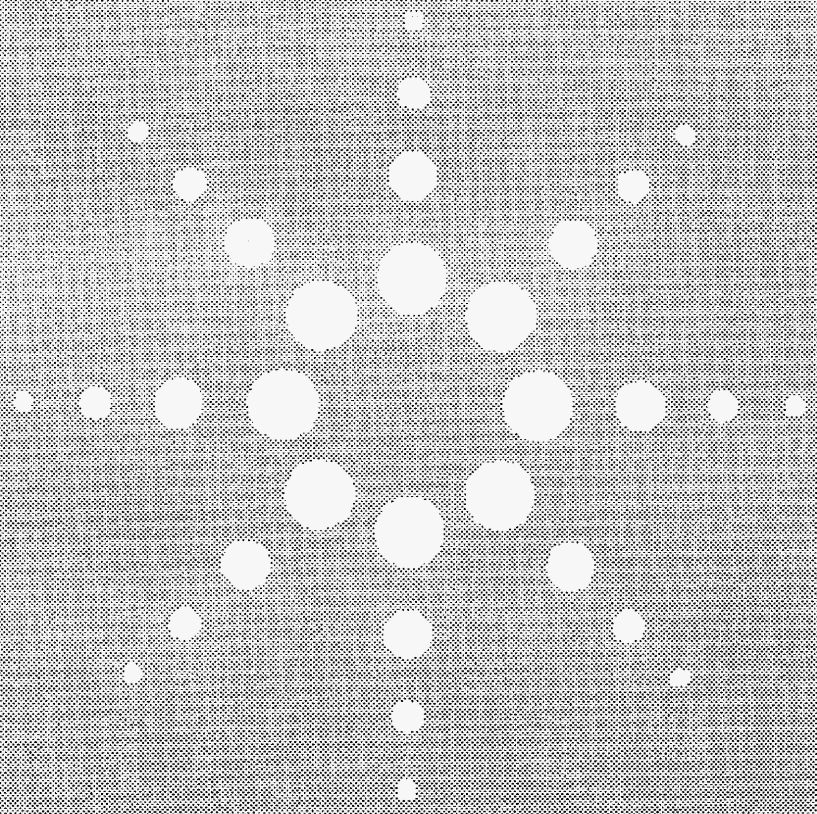
Agilent acceSS7

Business Intelligence



Obtain unique insight into your network and traffic

Agilent Technologies



Agilent acceSS7 Business Intelligence delivers unique and valuable insights into every aspect of network and customer activity, helping you achieve immediate financial and strategic benefits as well as long-term competitive advantage.

Profiting from network knowledge

The pressures and demands facing all areas of the telecommunications industry today are huge. The impact of regulatory changes, the explosive growth of the Internet, the migration to IP and other new technologies and increased customer expectations combine to create significant challenges. To survive and succeed in this intensely competitive environment, you need the power and flexibility of Agilent acceSS7 Business Intelligence.

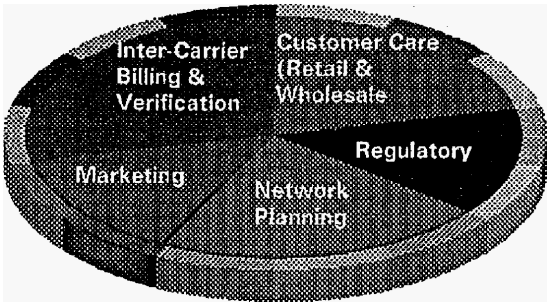
Agilent acceSS7 Business Intelligence is the only system available today that can capture and deliver a complete view of your network and traffic. It collects and records details of every call made, tracked from source to destination. It gives you details on calls to and from interconnecting carriers and covers successful, failed and unanswered calls. And it does all this reliably and unobtrusively, without impacting network performance in any way.

Agilent acceSS7 Business Intelligence enables many different business units within your organization to extract relevant information from a database record of network and customer activity. The benefits are substantial and far reaching. Equipped with hard facts rather than tentative estimates or approximations, you can plan ahead more effectively, improve your customer service and dramatically increase your revenues.

In summary, Business Intelligence provides full call analysis data to:

- Reduce network congestion
- Maximize new and existing service revenues
- Strengthen accuracy of interconnect billing

The benefits are of increasing importance in today's competitive environment in which network operators fight to retain and gain new network subscribers.



Making information work for you

Agilent acceSS7 Business Intelligence helps many of your lines of business to make timely, effective and well informed decisions. It brings together a wide range of decision support applications, development tools and consultancy services to analyze and report on calls handled by your network. You can depend on fast, accurate, cost-effective information, presented clearly and to the level of detail you require - the ideal basis for making sound business decisions and achieving substantial financial returns.

Interconnect Billing and Billing Verification

Agilent acceSS7 Business Intelligence provides the data necessary to ensure accurate inter-carrier reconciliation reflecting the true volumes of originating, terminating and transiting traffic.

- New revenue generation
- Accurate interconnect billing data
- Reduced outgoing payments

Marketing

Agilent acceSS7 Business Intelligence provides accurate measurement of service usage, so enabling immediate impact analysis of new services and promotions.

- Target new services for maximum revenue

Regulatory

Agilent acceSS7 Business Intelligence enables the automatic generation of network and service performance data required by many regulators.

- Demonstrate regulatory compliance
- Provide data on impact of non-compliance by other network operators

Customer Care

Agilent acceSS7 Business Intelligence lets you measure network performance (both in your own network and inter-connected networks) as experienced by your customer.

- Improve quality of service
- Analyze and minimize failed calls, including call completion ratio
- Select inter-connect partners based on measured past performance
- Police & inforce inter-carrier Service Level Agreements

Network Planning

Agilent acceSS7 Business Intelligence gives you a full account of network traffic to:

- Reduce network congestion
- Identify and solve network hot spots
- Minimize operational costs in the legacy network
- Target the deployment of new network equipment for maximum impact and minimum investment
- Improve quality of service
- Identify ISP traffic for data-offload strategies

Business Intelligence Infrastructure

SS7 messages are fundamental to the set up of calls in a modern digital network and control all aspects of communication between switches. Agilent accuSS7 Business Intelligence produces Call Detail Records (CDRs) by processing the individual messages. CDRs derived from SS7 are intrinsically more useful than CDRs generated by switches in a number of ways.

SS7 Call Detail Records	Typical Switch Call Data
Data collection is independent of the network elements and does not affect their performance	Data collection is dependent on the switches and may compete for processing resources with other functions, such as switching traffic
Data is collected and presented in a consistent format	Data collection is dependent on the switches and may be presented in vendor-specific formats, with each element type providing a different subset of the required data
Includes details on parts of the network not normally available, such as calls to and from interconnecting carriers	May not include these details
Includes details of every call made, including failed and unanswered calls	Does not generally cover statistics on failed calls
Includes information on call routing, covering terminating and originating information	Does not provide call routing or terminating call information
Covers the whole call, including call and transaction information provided in instances such as 1-800 or Local Number Portability (LNP) calls	Records only parts of the information relating to the call
CDR data can be made available while the call is still in progress, and in real-time upon call completion	CDRs are typically only available, at best, 15 minutes after the call has been completed, and sometimes only 24 hours later

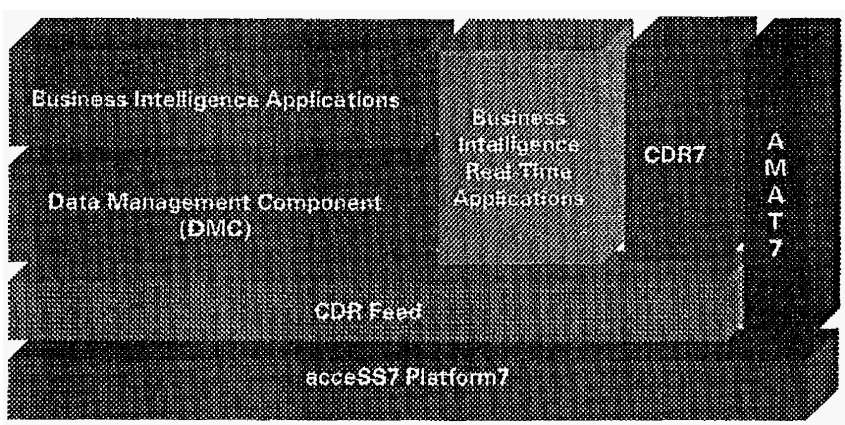
The acceSS7 Business Intelligence provides all the necessary automated collection, transport and management of SS7 CDRs to enable you to take advantage of this rich data source.

acceSS7 CDR Feed

Agilent acceSS7 CDR Feed is the foundation of the Business Intelligence infrastructure. It allows you to configure, manage and control the collection and delivery of CDRs from the SS7 network. It enables data collections from a small number of sites or network-wide. It can also be set up to feed one or more Data Management Components, where the data is stored. This lets you direct the data at a number of separate yet concurrent analysis tasks, each targeted at a specific business unit. CDR Feed offers a range of data delivery modes for real-time and mission critical data.

Data Management Component (DMC)

This component provides the data storage and management for CDRs delivered by the CDR Feed. It provides a consistent open interface for a wide range of acceSS7 Business Intelligence applications, enabling them to be designed independently of the underlying network infrastructure. These applications can be developed in-house or by Agilent partners. The DMC can deal with large volumes of continuous data while carrying out extensive integrity and cleansing tasks. Application and user waiting time is cut to a minimum; user applications can query the data with new CDRs integrated seamlessly as soon as they are received.



Business Intelligence Applications

Agilent accoSS7 Business Intelligence includes a set of standard applications designed to deliver immediate financial and strategic benefits. Our open approach enables additional custom-built solutions to be designed and deployed rapidly where standard products do not provide the functionality required. A number of partners are currently developing specialized applications for the Business Intelligence platform.

Business Intelligence are the components that turn raw data into vital business information. Most of them sit on top of the DMC and process the CDR data in large batches, typically every 24 hours. However, some requirements can only be met with data available in real-time. This can be done in a controlled near-real-time mode through the DMC, with batches typically being of five minutes, or in full real-time mode with a direct feed from the CDR Feed. Some of these applications are described below.

ISP Finder

Identifies ISPs on your own network and on interconnected networks by matching the call profile of every called number against the typical profile of ISPs. This data can be used for interconnect billing & verification and for network planning purposes.

Benefit

* Identify a major source of network congestion

Interconnect Analysis

Direct, accurate measurements of inter-carrier traffic are created, with measures of total calls and total MOU for each jurisdiction (e.g. local, toll, etc.). Bills and Rating Factors submitted by interconnecting carriers for jurisdictional reporting on originating, terminating and transit traffic can be validated and hard evidence provided with which to challenge estimates.

ISP traffic can be identified and reported separately, which supports both separate rates for ISP traffic and the generation of data with which to build a case for ISP tariffs.

Additional optional modules enable the accurate measurement of transit traffic across the network, giving detailed measurements by originating-terminating carrier combination; the separate measurement of pre-dipped toll-free traffic; the identification and separate reporting of all traffic to and from unbundled and resold lines in your network; and a variety of additional reports addressing such issues as volumes of MF interworking and No CPN delivery.

Benefits

* Carrier-specific measurements of all interconnect traffic
* Originating, terminating and transit measurements
* ISP traffic reported separately
* Reduced bills from other carriers
* Avoid terminating charges for transit traffic
* Avoid terminating charges for calls from unbundled and resold lines

Call Performance Manager

Provides detailed data on the call completion performance of interconnected carriers, including performance to specific destinations and services identified by leading digits. Real-time data is subject to thresholds, with alarms raised when these are breached. Carrier and destination specific historical records are also created.

Benefits

- Carrier, destination and carrier/destination combination measurements
- Thresholds applied against ASR and traffic volume
- Reroute traffic in real time to avoid congestion and failures in other networks
- Effectively police and enforce interconnect call service agreements
- Demonstrate call completion performance to other carriers and to regulators
- Select wholesale partners on the basis of measured performance

Traffic Analysis

Provides detailed analysis of traffic flows between parts of your network, or between parts of your network and other networks. Analysis by geographic region, with inter- and intra- region measurements for up to four sets of entities, for example, region, state and city measurements

Benefits

- Detailed traffic flow measurements for network planning
- Point-to-point measurements help identify congested nodes and possible solutions

CDR7

CDR7 makes quick cost effective voice trunk usage a reality. It captures real time billing data from the SS7 network and generates a Call Data Record (CDR), which it converts into Bellcore Automatic Message Accounting Format (BAF) records for sending to the downstream billing system.

Benefits

- Full payment for resource consumption
- Verify your interconnect charges
- Instant delivery of more accurate billing data
- Increased security for your bottom line
- Compliance with industry standards
- Near real time records

AMAT7

Automatic Message Accounting Transmitter for SS7 (AMAT7) makes quick,cost effective SS7 usage measurement a reality. It captures real time usage data about your SS7 network and converts it into a usable format so you can precisely measure traffic volumes and network conditions. It then groups the messages into accurate summaries, so you know exactly when and at what volume your network resources are being used.

Benefits

- Correctly dimension your signaling network
- Full payment for resource consumption
- Control the use of network resources
- Access to key marketing information
- Flexible measurement aggregation
- Compliance with industry standards

Future Applications

Agilent and its partners are constantly developing new applications to take advantage of the wealth of data that can be extracted from the SS7 network. As new challenges arise, new solutions will be deployed to meet them.

Partner Solutions

Not all the acceSS7 Business Intelligence applications are developed by Agilent. Through our partner program we work with other companies to deliver a wider range of applications than we could do ourselves. The open architecture of the acceSS7 Business Solution facilitates the development of applications by third parties. Most of our customers have developed and deployed their own custom applications on the DMC.

Call Performance Manager is an example of a partner application. It is developed by Eiron TeleSoft, a provider of high-value intelligence for the telecommunications industry.

Global Communications Services

The Agilent Technologies acceSS7 network monitoring system provides detailed, accurate insights into every aspect of network activity in real time by exploiting the valuable information in the SS7 network. Agilent acceSS7 has become the network monitoring market leader, offering and deploying the most advanced and broadest set of applications in the industry. Agilent acceSS7 benefits all business units in a network operator with applications covering surveillance, troubleshooting, fraud management, billing data collection and business intelligence. We are the world's largest telecom test equipment company. Our in depth knowledge of the telecom industry and marketplace, combined with our expertise in computers and networking, test and measurement solutions and communications technology, places us and our partners in a unique position in this rapidly expanding market.

Agilent acceSS7 Business Intelligence is the only solution available today that can give many business units within your organization comprehensive, robust and accurate information about what is happening on the network. It can deliver immediate and substantial financial returns. Make it a key part of your business strategy.

Agilent Technologies' Support, Services and Assistance

By internet, phone, or fax, get assistance with all your communications needs.

Online assistance:
www.agilent.com/find/assist or for specific Agilent acte537 information www.acte537.com

Phone or Fax

United States:
(tel) 1 800 452 4844

Canada:
(tel) 1 877 894 4414
(fax) (905) 206 4120

Europe:
(tel) (31 20) 547 2323
(fax) (31 20) 547 2390

Japan:
(tel) (81) 426 56 7832
(fax) (81) 426 56 7840

Latin America:
(tel) (305) 267 4245
(fax) (305) 267 4286

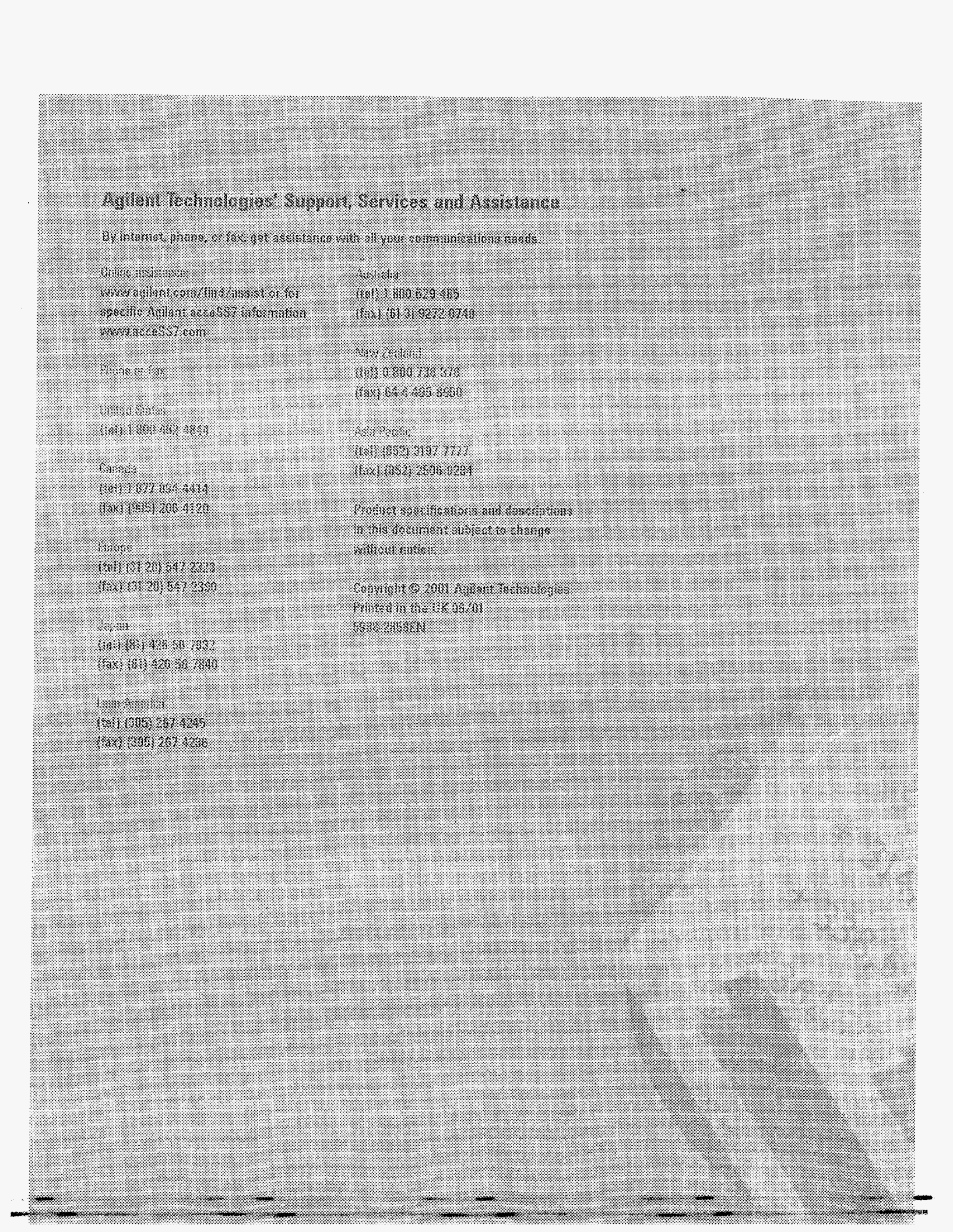
Australia:
(tel) 1 800 629 485
(fax) (61 3) 9272 0749

New Zealand:
(tel) 0 800 738 378
(fax) 64 4 495 8950

Asia Pacific:
(tel) (852) 3197 7777
(fax) (852) 2506 9284

Product specifications and descriptions in this document subject to change without notice.

Printed in the UK 06/01
5980 2858E/N



Docket No. 041144-TP
Exhibit ___ (WLW-2)
Access Bypass study results

CONFIDENTIAL

Docket No. 041144-TP
Exhibit ___ (WLW-3)
Agilent CDR's

CONFIDENTIAL

(On CD Only)

STATE OF KANSAS

COUNTY OF JOHNSON

BEFORE ME, the undersigned authority, personally appeared Dr. Brian K. Staihr, who being duly sworn deposes and says:

That he is a Senior Regulatory Economist for Sprint Corporation. That he developed the random sample of call details records contained in Exhibit WLW-4 related to the traffic KMC delivered to Sprint over KMC's local interconnection trunks for termination by Sprint. That he chose the days for the sample through random number generation, using the months beginning November 1, 2002 and ending January 31, 2005. That this time period involved 823 days at 24 hours a day, which equaled 19,752 population hours. That one day per month (or 27 days) at 24 hours per month equates to 648 sample hours. That a sample size of 648 with a population of 19,752 (the equivalent of a statistically infinite population) produces results at a 95% confidence level and a .04 confidence interval. That this confidence level and confidence interval together produce a statistically valid and representative sample.

WITNESS my hand and seal this 28th day of February, A.D. 2005.

Signature _____

Debbie K Draper
Notary Public
State of KS

My commission expires: June 4 2005

Docket No. 041144-TP
Exhibit ___ (WLW-5)
KMC CDR Records

CONFIDENTIAL

(On CD Only)