Agilent Technologies

Service Provider Revenues: Recovering Lost Profit

October 23, 2002

presented by:

Colin Yates, Vodafone
Elaine Eisner, Cerebrus Solutions
Patrick Leask, Agilent Technologies

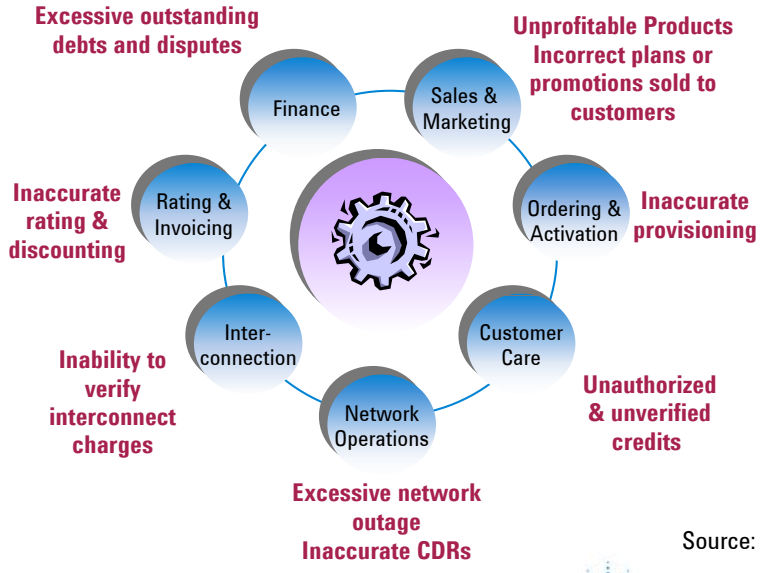
Revenue Assurance & Fraud Today

Revenue Leakage

“33% of companies don’t know if they have a revenue leakage problem”

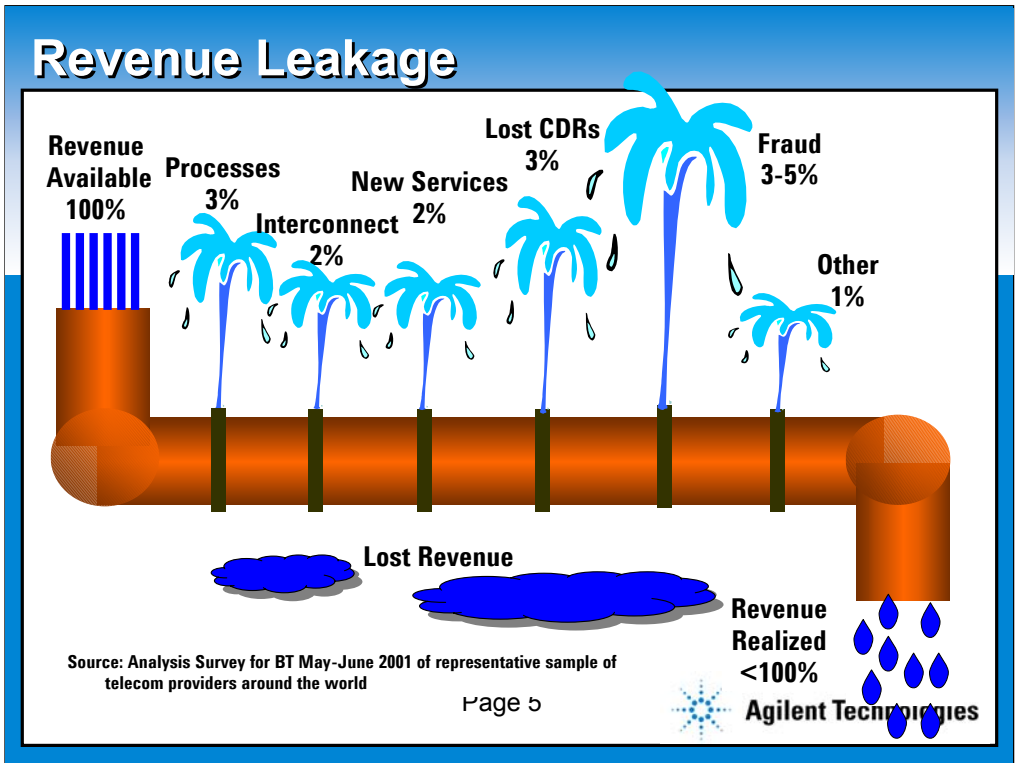
- Survey by Deloitte & Touche

Sources of Revenue Leakage



Source: PWC

Agilent Technologies



Turning to page #???, we can also use a “pipeline” metaphor for lost revenue.

In a perfect world, 100% of the potential revenue flowing through the Service Provider would be realised.

In reality, the 100% flow is reduced in many places by imperfections or inaccuracies in the business data, tools and processes.

Visualizing these as “leaks” in the pipeline, we see, for example, that inaccurate compensation between service providers at the Interconnects can cause up to 2% of potential revenue to be lost.

Lost CDRs can cause up to 3% of potential revenue to leak away, these can be attributed to a number of causes, for example incorrect, inaccurate or duplicate CDRs detected during the mediation process.

One example of CDR Loss I’ve encountered at a service provider was where billing for a whole trunk group was accidentally disabled due to a configuration error, but not discovered for a number of weeks.

As we can see from our pipeline, one of the biggest causes of lost revenue is Fraud, where various industry analysts reckon that between 3% and 8% of revenue is lost for the average service provider.

An average revenue loss for most service providers is about 5%- most will lose revenue via all of these common causes, but not all to the same extent.

I’ll hand back to Colin now, for a discussion on the major source of revenue loss shown here- Fraud.

Fraud Overview

- Fraud opportunities have increased over the years
- Losses vary depending on who you talk to
  - FIINA says $55Billion
  - CFCA says $12 billion
  - Others say between 3 & 5% of revenue
- Only certainty is that losses are significant

Fraud Overview

- Industry has gone through incredible change
- Staff levels, margins and profits have dropped
- More emphasis on reducing costs
- Looking at what value fraud management & revenue assurance programs can add
- Today will outline major fraud and revenue assurance issues facing the industry
- Will offer advice and solutions on how to identify and mitigate these revenue risks.

Fraud Overview

- Never a more appropriate time in our industry to take action against revenue leakage
- Fraud management and revenue assurance disciplines are now closely aligned
- Experience has proved that revenue assurance is major beneficiary of an FMS.

How much has fraud really changed?

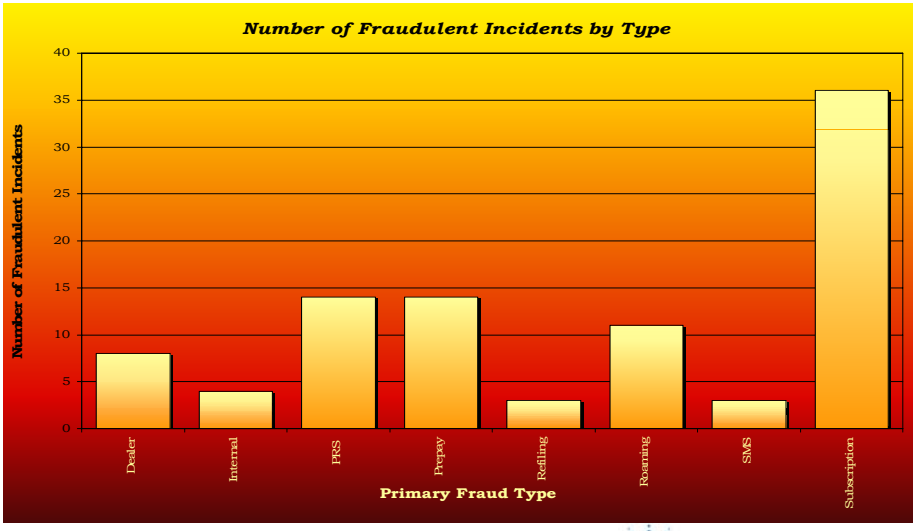
- During mid-90's, major changes predicted
- Internet & VOIP were going to change the fraud profile
- Most fraud issues from 90's still here today

How much has fraud really changed?

- A survey completed in 1996 identified the major fraud concerns as:
  - Subscription fraud
  - Premium rate service fraud
  - Cellular cloning
  - Clip-on fraud
  - PBX fraud

How much has fraud really changed?

A survey completed in Sept 2002 (mobile operators)



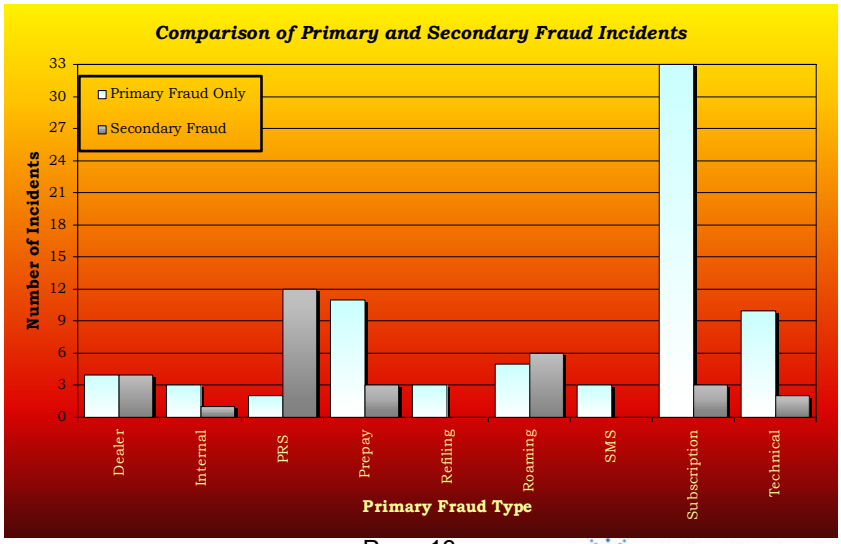
Agilent Technologies

Subscription Fraud

- Fraudsters drivers remain the same
- Service providers exposure has increased
- Generally results in a secondary fraud such as PRS, roaming or call sell
- Recent survey: 32 incidents reported had 23 incidents of secondary fraud
- Will remain a significant risk in the future

Subscription Fraud

- Secondary fraud as a result of subscription fraud



Agilent Technologies

Premium Rate Service Fraud

- Information provider stimulating calls into his service to inflate revenue
- Technology has increased opportunities for fraudsters to commit this type of fraud
- Fraudsters will generally not defraud the network provider who is hosting their service

International Resale Fraud

- Now a major problem world-wide
- Fraudsters establish a business relationship
- Offer discounted prepay services
- Pay first 2-3 months accounts then dispute
- During dispute reduce their call rates - increase their business and their debt with Operator
- Will disappear when recovery action threatened
- Will then move across border to next victim
- Losses large - generally $5 to $10 million

International Resale Fraud

- Some recent “actual losses” though IRF:
  - Belgium July 2001 - $1.5 million
  - Canada Mid 2001 - $700,000
  - Denmark Jan 2002 - $1 million
  - Russia July/Aug 2002 - $3 million
  - Greece July/Sept 2002 - $7 million

Roaming Fraud

- Opportunities increase as service grows
- Subscriptions obtained with false ID
- SIMs taken across international boundaries
- Used for Call Sell Operations
- Losses are generally high
- Dependent on receiving HUR from VMNO
- GSMA now working towards NRTRDE

Other Fraud Causing Major Risk

- PBX Fraud
  - Still a major vehicle for ‘Call Sells’
- Clip on Fraud
  - Increased incidents since 9/11

What now? A Few Conclusions

- Telecommunications fraud here to stay
- Fraud remains significant business risk
- Most frauds result in ‘hard currency’ losses
- Effective fraud detection tools mandatory for service provider success
- Recent industry losses could put small operators out of business
- Equally important is an effective revenue assurance program

Before implementing RA Strategies…

- How secure are today's revenues?
- How much revenue is available for funding from existing networks and services
- How long before your network is attacked by a major fraud?
- What are complexities of new technologies?

Today's Revenue Assurance Technologies

Technology Overview

- Traditional technology:
  - Call detail reports from switches
  - Rules and thresholds
  - Call detail data mining
- Subscriber profiling and behavior analysis
- Signaling data feeds
- Hybrid solution includes all of the above

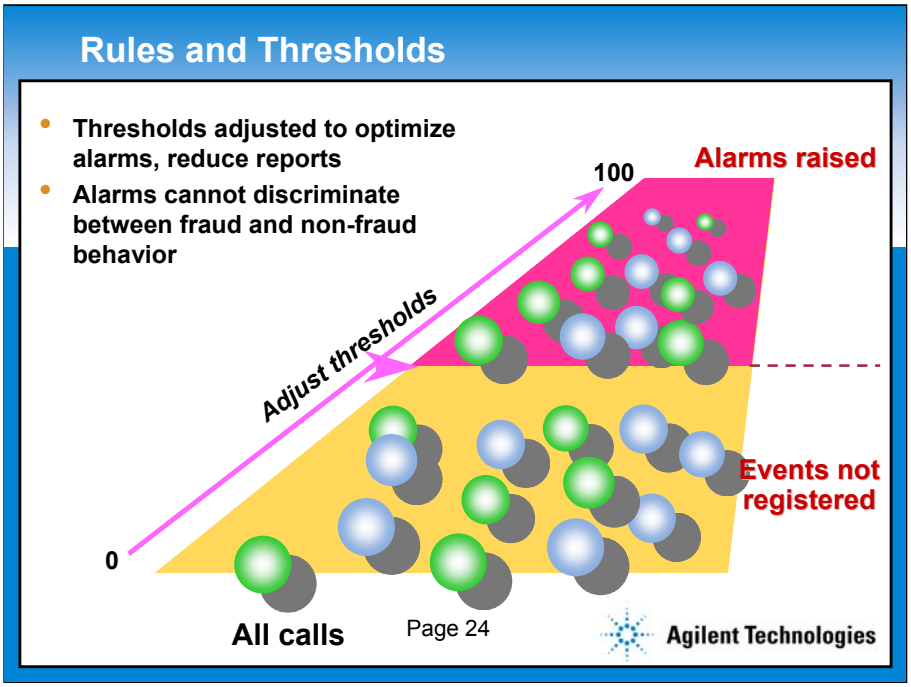
Call Detail Reports from Switches

- Laborious, time-consuming
- Searching for proverbial needle in haystack
  - Low “hit rate”

Agilent Technologies

Allow any changes to the system to be recorded – replace the Audit System log.

Of interest mainly to the Fraud Manager.



Effectively conventional systems divide the world into two groups:

A) All those fraudulent and non fraudulent calls which trigger thresholds and,

B) All those which do not.

The thresholds are set as a compromise between number of alerts raised (Sustainable workload) and detecting fraud.

Thresholds are indiscriminate, they cannot tell the difference between good and bad subscribers who trigger the thresholds.

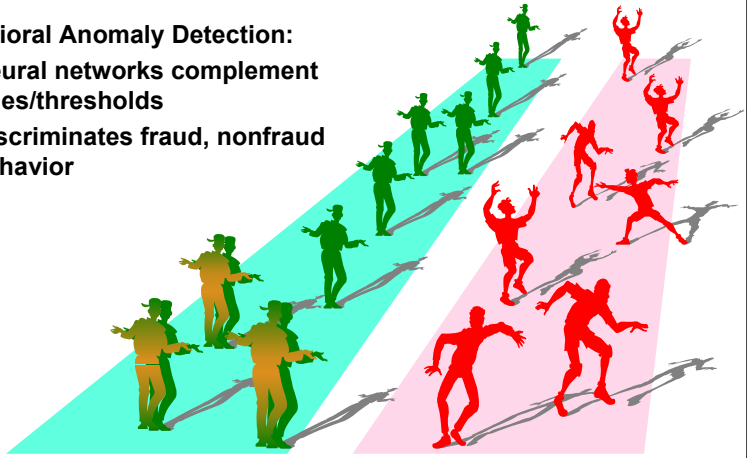
Call Detail Data Mining

CDRs

- Evolutionary step in technology
- Quickly access detail in call records
  - Relationships and linkage

Subscriber Profiling & Behavior Analysis

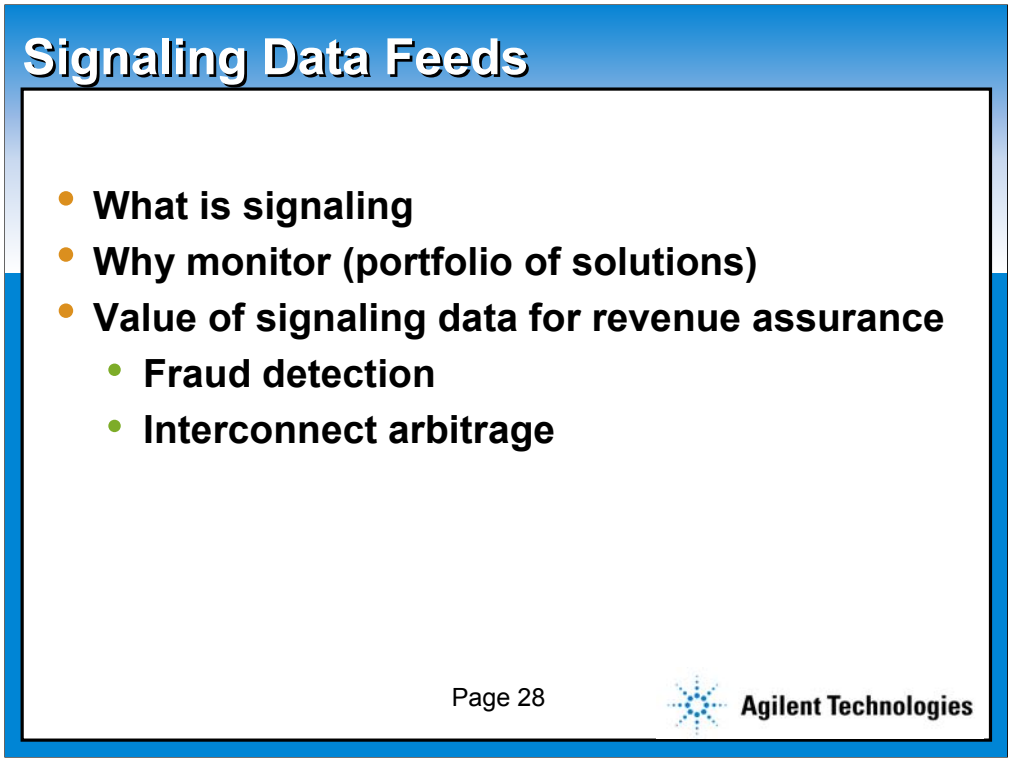
- Behavioral Anomaly Detection:
  - Neural networks complement rules/thresholds
  - Discriminates fraud, nonfraud behavior



Good Behavior

Fraudulent Behavior

Real-time Revenue Assurance & Fraud Management

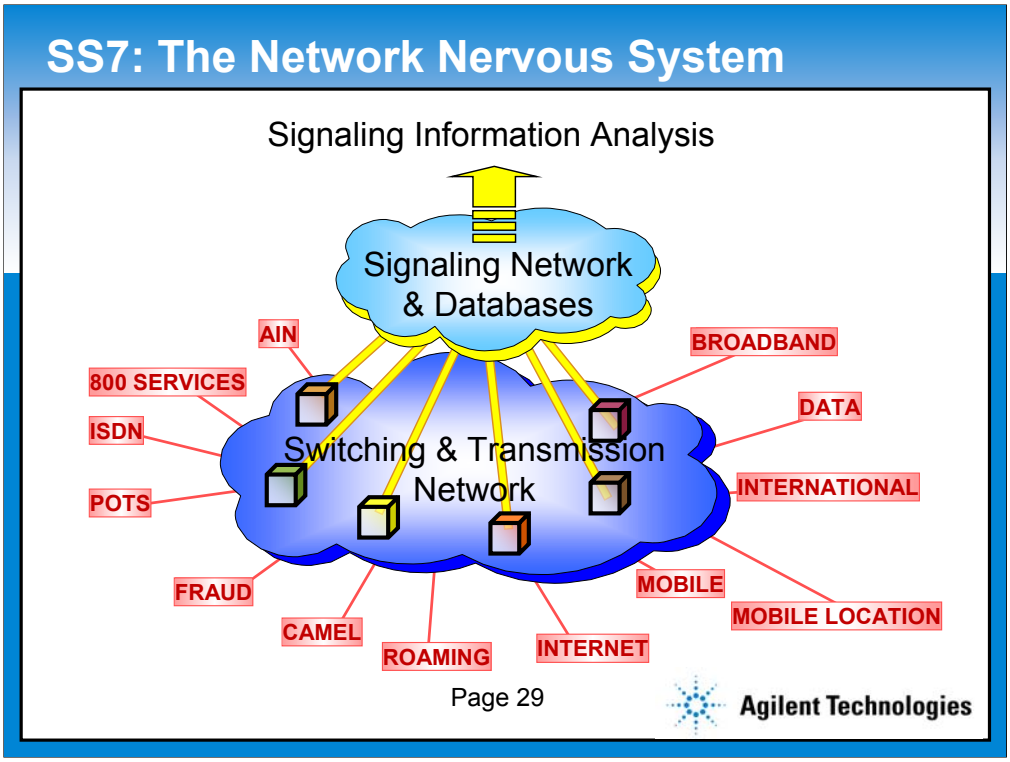


Elaine has just described some techniques used to analyse and process data for fraud detection, but the fraud information generated from this raw data is only accurate, valuable and useful if there is an effective source of data in the first place.

Effective data needs to be timely, accurate and rich enough to be able to provide 3 important perspectives for analysis: a network view, a service view and a subscriber view.

I'd now like to discuss a source that provides such valuable data for detecting and monitoring fraud for a network or service provider: the network signaling data.

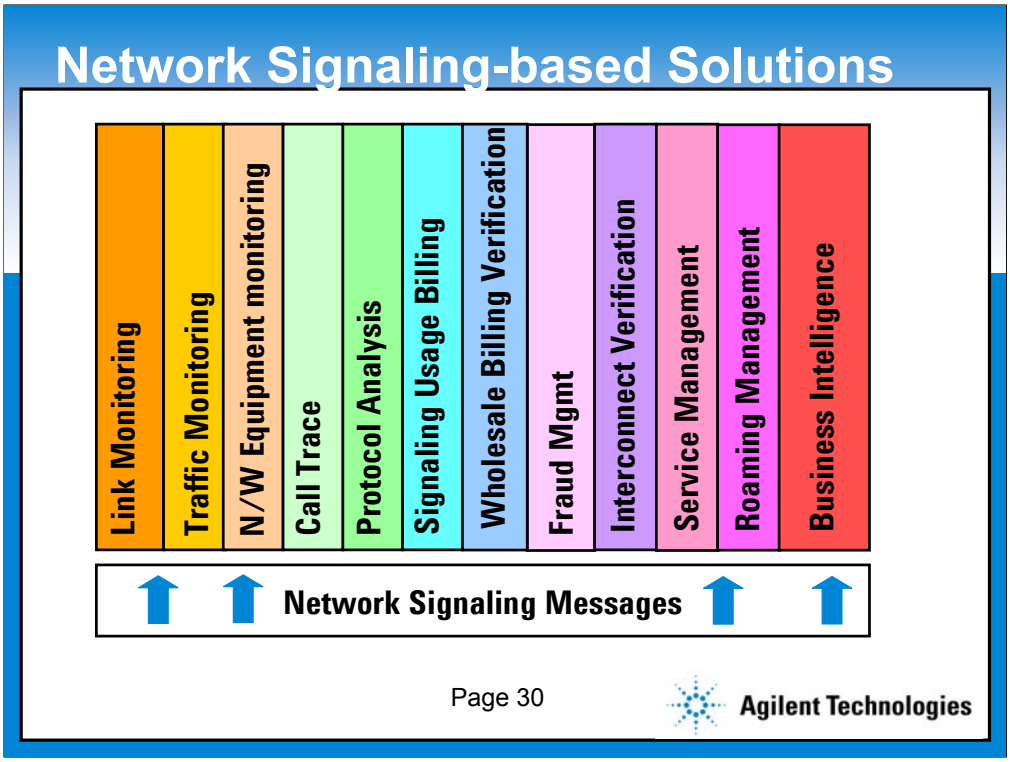
I'll talk a little about what we mean by signaling, why we would want to monitor it, and then describe the value that signaling-derived data has for finding sources of revenue leakage, along with a few examples.



The most common and pervasive form of network signaling used today is SS7, or Signaling System Number Seven. This has been around for over 15 years now, and was initially introduced to enable a national 800-number database service in the US.

Incidentally, another driver for SS7 was to combat fraud- some of you may remember the “black-boxing” type of fraud that was popular in the 1980s that involved sending signaling tones down the phone line to manipulate end-offices and switches- the aim being to avoid paying for the phone call. SS7 introduced “out-of-band” signaling, where the signaling between switches is carried on a separate physical link from the voice trunk- the caller is now unable to manipulate the network using the voice trunk.

As the diagram on page **???** illustrates , SS7 forms the heart of every phone network today. It’s used to provide a broad and pretty diverse range of services, from POTS (that’s Plain Old Telephone System) using basic call set-up and tear-down procedures, through to complex mobile authentications, handovers and subscriber roaming.



Looking at slide **???**, we can see a whole spectrum of ways we can use the signaling data to manage the network, services and subscribers.

By monitoring the signaling data, we can determine detailed performance data about the signaling links themselves, the network elements, the traffic carried by the network, and the performance of the full set of services that the network provides.

By collating the signaling from different parts of the network, we can abstract the raw data and generate Call Detail Records (CDRs). We can use these CDRs in the same way we use CDRs from the network equipment, but because the CDRs are derived from the signaling data they contain a richer set of information- we get a more comprehensive picture of how the network and services are performing, and we can find out a lot more about the activity of the subscribers in the network.

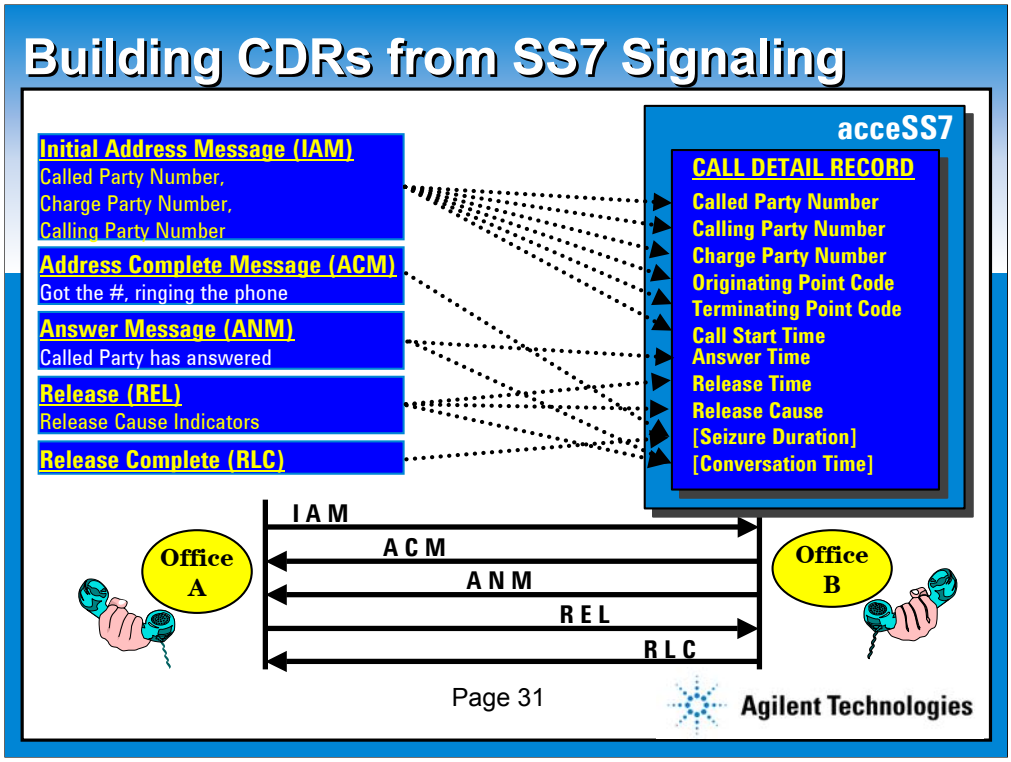
Some of the uses we can put these signaling-derived CDRs to include detecting fraud on the network, verifying inter-carrier billing, analysing the source, destination and type of interconnect traffic and monitoring the state of subscriber roaming services and roaming partners.

In addition to monitoring these essential services, we can feed the SS7 CDRs into a data warehouse, then “slice and dice” them to generate intelligence about the use of the network, services and subscribers.

Some actual examples of the uses operators make of this include:

- analysing the traffic patterns between end offices to determine the most cost-effective deployment of new voice trunks

- measuring the quality of service provided by interconnect partners in order to select the best routing for subscribers



How do we actually generate CDRs from signaling data?

Here's an illustration that shows how the signaling messages for a simple voice call can be used. We take each signaling message, and extract the valuable fields into a CDR. When the call is finished, we end up with a CDR containing a much richer set of information than an equivalent CDR from a network switch.

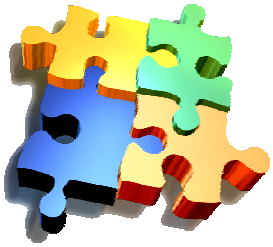
Value of Network Signaling Data

COMPREHENSIVE

- ✓ Correlates complex calls (AIN, 800)
- ✓ Captures calls switches don't (IC's)
- ✓ Shows abnormal call events (Unans)
- ✓ Can get roamer, mobile location data

EFFICIENT

- ✓ Consistent output format
- ✓ No need for complex mediation
- ✓ SS7 data is cheaper to collect
- ✓ Scalable, superior to sampling



ACCURATE

- ✓ Complete record of service usage
- ✓ Times call events precisely
- ✓ Available immediately (not batched)
- ✓ Provides in-progress call data

SS7 data is a necessary complement to switch CDRs for Revenue Assurance

Agilent Technologies

The next slide, page **???**, summarises the value of the signaling data.

The important points to note are that signaling data

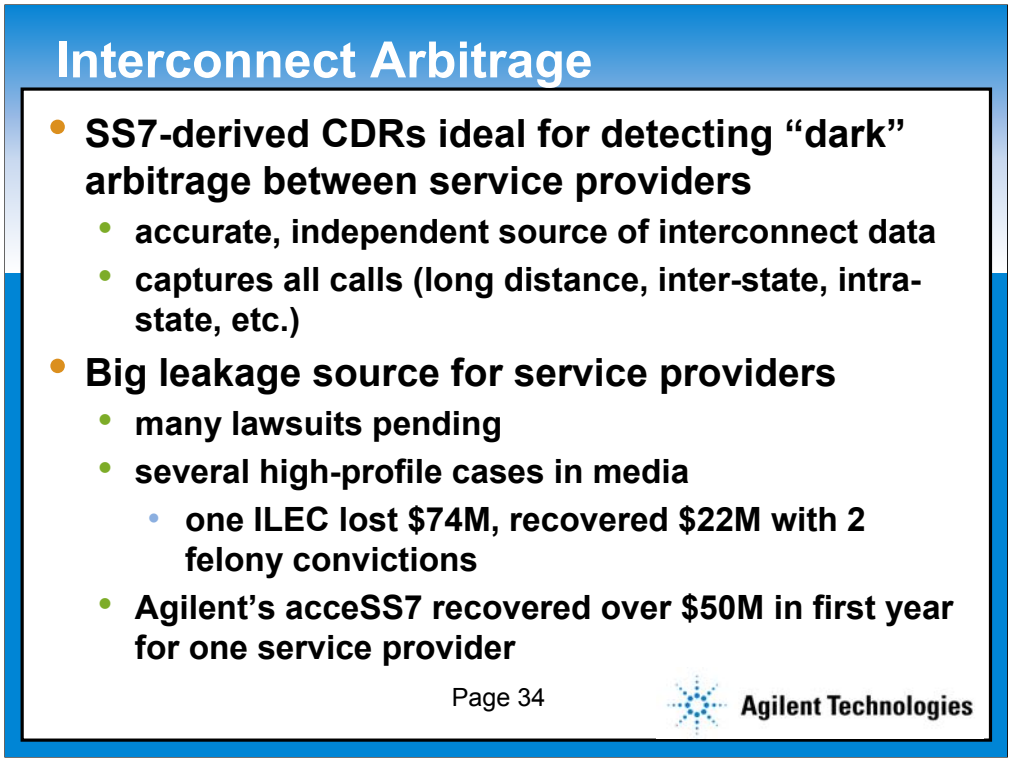
SS7 CDRs for Fraud Detection

Switch CDRs provide basic data:

- Outgoing calls
- Completed calls

SS7-derived CDRs also provide:

Extra CDR fields	3-way calls
	Carrier Surfing
	Call Forwarding
Untampered call info (pre-billing)	Insider Fraud
Unanswered calls	Call-back
Incoming calls	
Calls in real-time	Call Sell Operations
Calls in progress	Long duration calls
More accurate CDRs	All Fraud scenarios
	etc.…

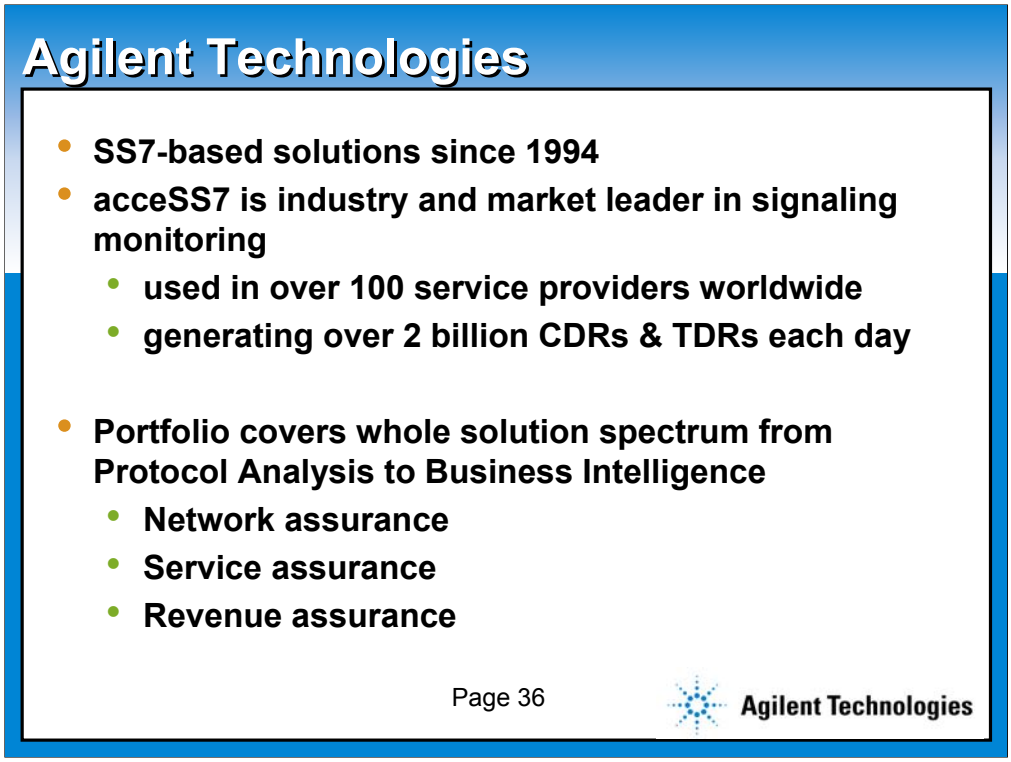


Closing remark to lead into Elaine again:

So we've seen that Signaling provides a valuable source of data for detecting and monitoring fraud on a Service Provider's network.

A key attribute for a Fraud Management solution is the ability to take data from a number of sources, such as S7 signaling, and to use several proven technologies to detect fraudulent behavior……

Agilent & Cerebrus Integrated Solutions

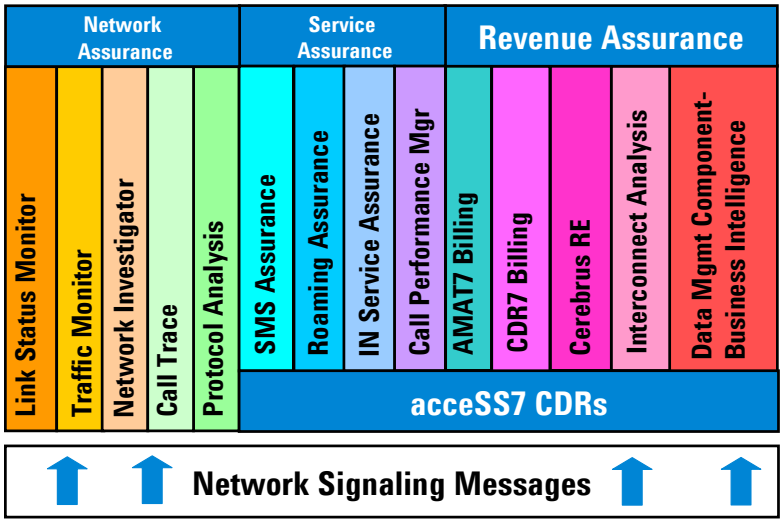


Agilent have been providing signaling data based solutions to service providers for over 7 years now. We have a proven and **reliable** platform for generating Call Detail Records from signaling data, in use for many mission-critical revenue and service assurance solutions today in over 50 network operators worldwide.

Scalability: from <5M/day to > 370M CDRs/day

Broad coverage- network technologies & services

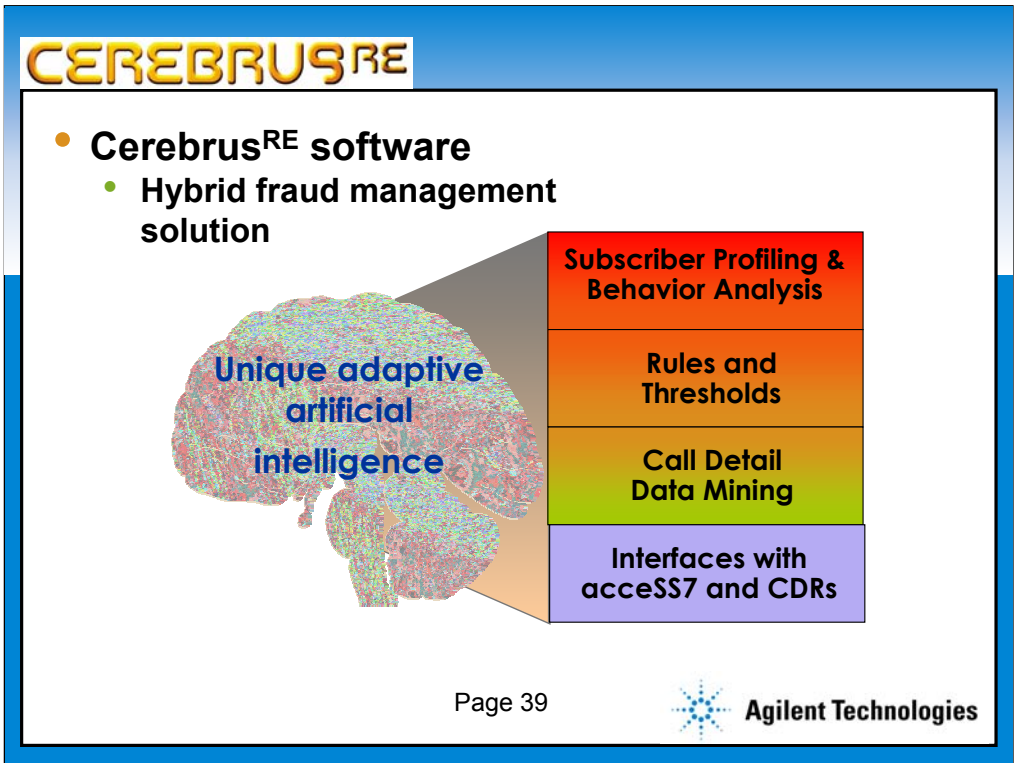
Agilent acceSS7 Solution Portfolio



Agilent Technologies

Cerebrus Solutions

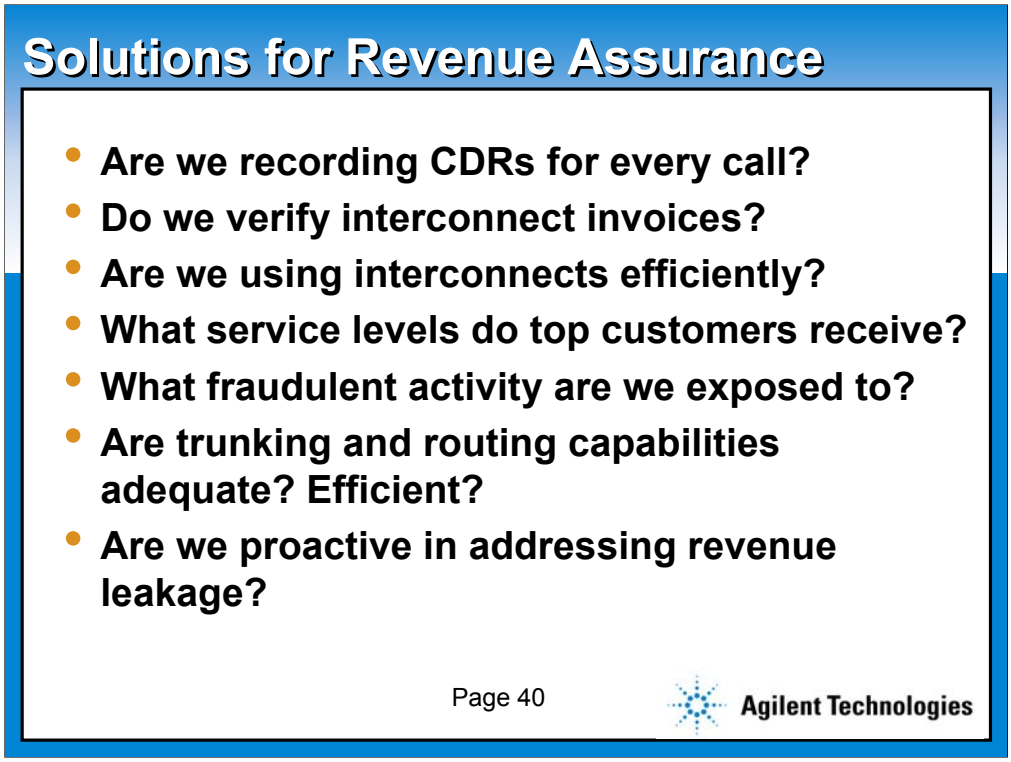
- Leading global provider of hybrid fraud management solutions for telecom industry
  - World class customer base on five continents
- Agilent a strategic investor
- Cerebrus^{RE} software
  - Flagship fraud management product
  - Integrates acceSS7 data feeds



If you give a good fraud manager a set of call detail records, just by studying the detail and patterns of the calls e.g duration, destinations etc., they will be able to identify those calls which have made them suspicious.Using their experience and expertise, they will identify certain fraudulent characteristics, which if observed will be indicative of a high probability of fraud.

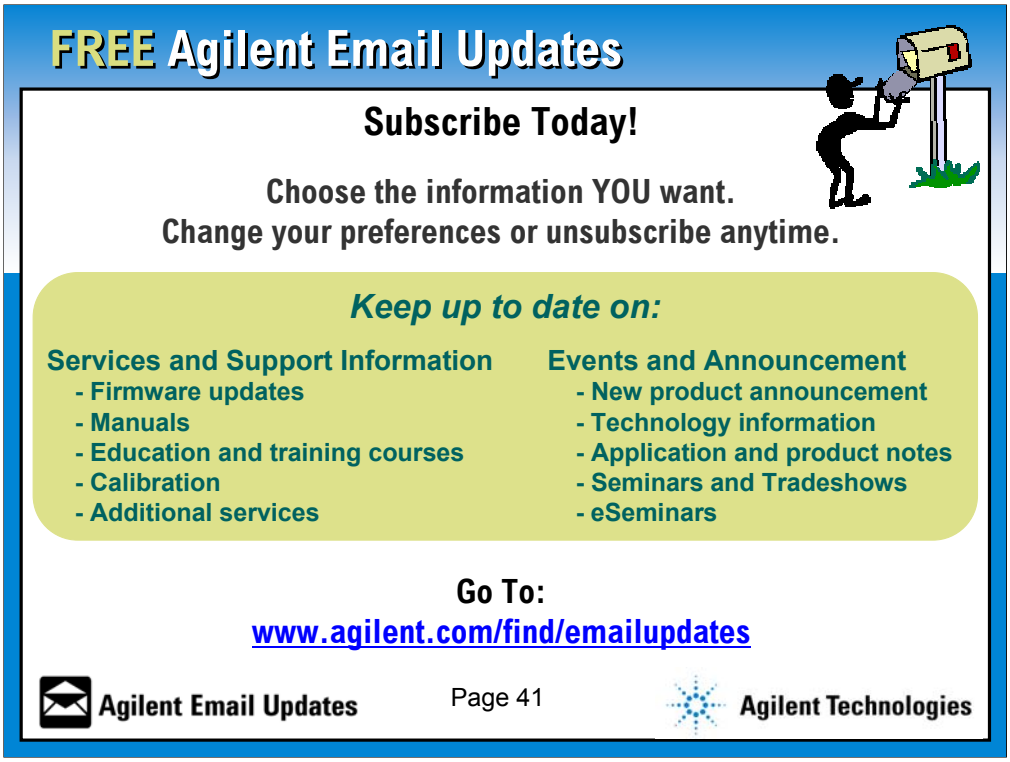
Cerebrus' neural based system is designed to act just like a top class fraud manager. The system looks at the call details and looks for suspicious activity, mimicking the way the fraud manager works. Cerebrus acts like an army of fraud managers detecting unusual behavior and behavior that is indicative of fraud. This allows the user to have fewer top class fraud experts (which are difficult to find) or to reduce the level of training involved for less experienced fraud analysts.

Another analogy would be the customer looking at their own phone bill. Because the customer has made the calls on their account, they can soon tell if there are any additional fraudulent calls they are being charged for. Cerberus' Neural Network works in the same way. It keeps a profile for each customer of the type and duration of the calls and the time of day and day of the week that each customer makes those calls. As new calls arrive for that customer, Cerebrus compares these to the calls the customer would normally make and then raises an alarm if there are 'significant' differences.



If you're unable to answer any of these questions, you may be among the 33% of companies who don't know if they have a revenue leakage problem.

If you can't answer all of them, your revenue is probably leaking away, and you're missing many valuable opportunities to contribute to your top-line revenue.



In a moment we will begin with the Q&A but 1st, for those of you who have enjoyed today's broadcast, Agilent Technologies is offering a new service that allows you to receive customized Email Updates. Each month you'll receive information on:

- **Upcoming events such as eSeminars, seminars and tradeshows**
- **the latest technologies and testing methods**
- **new products and services**
- **tips for using your Agilent products**
- **updated support information (including drivers and patches) for your Agilent products**

It's easy to subscribe and you can change your preferences or unsubscribe at anytime. Once you've completed the NetSeminar feedback form you will be directed to Agilent's resource page located on slide # XX, at that point simply click on the Agilent Email Updates link and you will be directed to the subscription site.

Now on to the feedback form then to Q&A……..