

**TERALIGHT, LTD.**

**“UNITING THE OLD WORLD WITH THE NEW”**



**TERALIGHT, LTD.**  
“UNITING THE OLD WORLD WITH THE NEW”

## Teralight Ltd. - Alliance with PTTs

**Teralight, Ltd.**, a seven year old company, headquartered in Dubai, U.A.E., is a Management Consulting and Technology products and services company with a business acumen specializing in:

- business development
- international telecoms regulatory matters
- network fraud detection and elimination
- market research
- infrastructure due diligence
- asset acquisition for leading IT and Telecommunications organizations in Pakistan and in MENA.



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Teralight Locations and Facilities

- **Corporate Headquarters:**  
Level 41, Emirates Towers  
P.O. Box 31303  
Sheikh Zayed Road  
Dubai, UAE  
TEL# 971.4.319.9173
- **Pakistan Headquarters Office**  
Software Technology Center  
Third Floor, Suite 305C  
Evacuee Trust Complex  
305A Agha Khan Road  
Islamabad, Pakistan  
TEL# 92.51.287.6272
- **Pakistan TASC/TNT:**  
32-Empress Road  
1<sup>st</sup> Floor, Ferozsons Building  
Lahore, Pakistan  
• TEL# 800-959.2733
- **Hong Kong Office**  
Bank of China Tower  
1 Garden Road, 25th Floor  
Central, Hong Kong, China  
TEL# 852.2251.1888

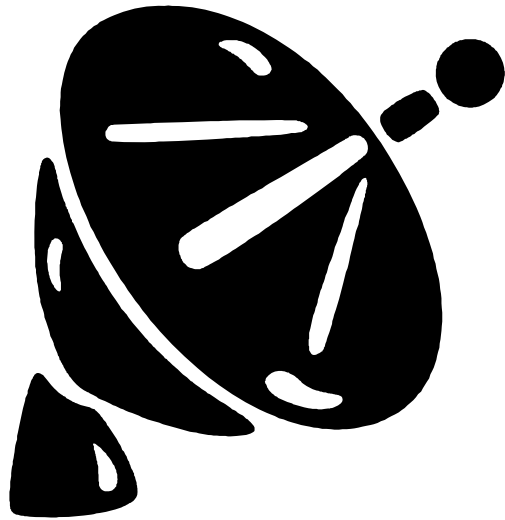


## Fraud Detection & Revenue Assurance

- Network Fraud Detection and Revenue Assurance Planning (**Guardian Data, Guardian Detect, and Guardian Voice & Data**)
- Build pro-active measures to eliminate illegal access to the network
- Modular approach to fraud detection via Billing, SS7, and Manual Mechanics. Must find way to monitor both ends of calls.
- Intl Bypass Fraud costs Operators hundreds of millions of \$ per year
- There are some very easy and simple ways to detect and STOP this activity
- Carriers must learn how the bypass network owners think and operate in order to be able to challenge them and eliminate their associated revenue depleting routes.



## Teralight Ltd – Types of Frauds



- Calls and Message Traffic Selling Fraud Activities
- Fraud Information Exchange and Distribution over the Internet
- Insider Oriented Fraud and Collusion
- Interconnect Bypass (International Usually) Fraud
- International Roaming Fraud
- Network Systems Hacking
- Premium Rate Service Fraud
- Sales Distribution and Agent Fraud
- Subscription Fraud and ID Theft



## How Bypass Fraud Hurts Pakistan

- Pakistan Economy is growing strongly for the year end 2004.
- Pakistan is now going through certain privatization efforts.
- Bypass Network Owners only pay to PSTN, local termination costs for their international minutes which should be charged at the International Rate.
- Reduced profitable revenue depresses share holder value!
- Network utilization by Bypass companies destroys planned management of facilities.
- Tandem switching systems are not used, but local Centrex's are, therefore causing undue stress on local facilities.



## Bypass Damages to Revenue

- In Pakistan, local city termination is used by Bypass Networks
- Local termination calls are one time charge per call:  
2 rupees = \$.034/call
- Local mobile termination costs are charged only:  
2.8 rupees = \$.04732/min
- Average length of call is approximately 4 minutes in length
- The legal minimum rate per minute for Intl. inbound is \$.125 US
- A 4 minute call locally would bring \$.50 to PSTN at minimum if legal
- A 4 minute Bypass call brings only \$.034 to PSTN. A difference of \$.466
- A 4 minute Bypass call to mobile brings \$.189 to PSTN. A diff of \$.311



## Bypass Damages to Revenue

- Average Bypass Site number of Lines – 60 to 90 lines
- Average Usage is very high – 15,000 minutes per month per voice line
- Average Traffic per E-1 connection is 450,000 minutes per month or more
- Assuming that each site is 60 lines each, the PSTN carrier can stand to lose;

- 
- One Site of Local Lines (Typically Karachi, Lahore or Islamabad)

equals **LOSS** of US                    **\$419,400** per month per 60 line site

equals **LOSS** of Rps                    **R24,744,600** per month per 60 line site

- One Site of Mobile Termination

equals **LOSS** of US                    **\$279,900** per month per 60 line site

equals **LOSS** of Rps                    **R16,514,100** per month per 60 line site



## Bypass Damages to Revenue

There are an estimated fifty (50) sites or more in Pakistan

### TOTAL ESTIMATED DAMAGES to REVENUE

- 25 Sites of Local Term. COSTING LOSSES of \$10,485,000 monthly  
Equals est. losses on an annual basis of \$125,820,000
- 25 Sites of Mobile Term. COSTING LOSSES of \$6,997,500 monthly  
Equals est. losses on an annual basis, \$83,970,000

TOTAL LOSSES ESTIMATED @ \$209,790,000 PER YEAR!!!



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Typical Billing System Tools

- Call Detail Record (CDR) Mediation
- Data Clearinghouse Activities
- Suspense files of suspect Accounts
- Rating Functions of the Billing System
- Billing Functions of the Billing System (Invoicing)
- Advanced Reporting Methods
- Exception Reports



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

# Typical Fraud Management Scheme

Clearing House  
SDRS-IP/SS7/SMS/etc  
Customer Master Index  
Billing Payments  
Applications of Service  
Service Changes  
Marketing Promotions  
Credit Limits  
Debit Cards

SYSTEM PROFILE

Intelligent Networks

Bad Debt

Sub Fraud

Technical Fraud

Access Fraud

CATEGORICAL REFERENCE

Fraud Systems check all possible data

Fraud Systems will check results

If no Fraud is detected, then record is ok

If Fraud is detected, then Record is

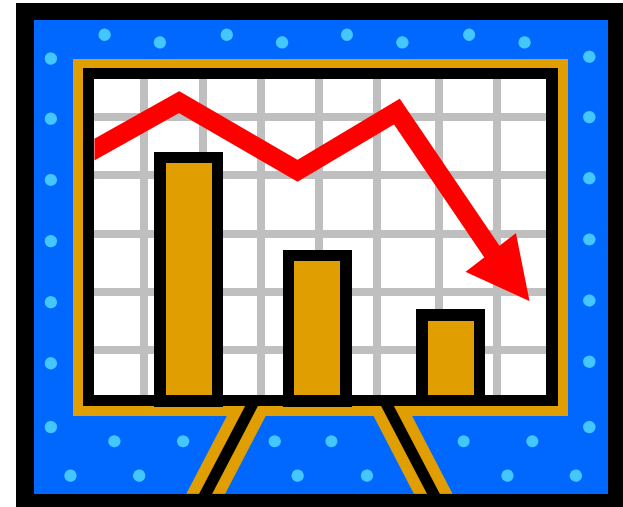
sent for company analysis



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Bypass Fraud is very Expensive

- Operators either fixed or mobile experience between 1% to 3% of their revenue being from fraudulent activities
- Roaming Fraud is currently an estimated 24% of total fraud – GSM Association
- Fraud represents a number as high as 50 to 65% of the total bad debt of a carrier's revenue
- Handset usage losses from roaming Fraud can be as high as \$12,000 per day.
- Interconnect Fraud costs service Providers hundreds of millions of lost revenues on an annual basis
- Interconnect Fraud can be stopped in its tracks but it requires teamwork from all participants, regulatory bodies, operators, consultants and others!



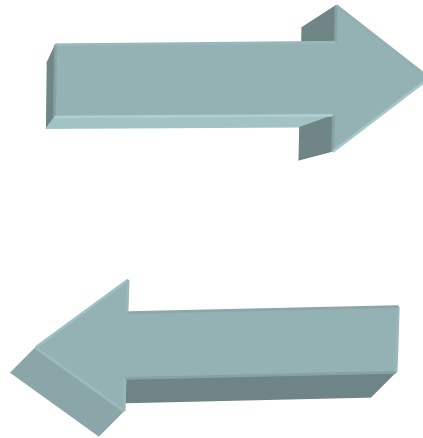
# Techniques for Wireless Roaming Fraud

## Operator - X

1.) Fraudulently obtain Subscriptions from Operator X.

Subscription Fraud  
Dealer Fraud  
Internal Fraud  
Technical Fraud

2.) Ship, Steal Handsets to distant operator Z



## Operator - Y

3.) Utilize subscription in high Value markets, running up billing charges.

Call Selling – Cards, pins, etc.  
Call Selling – International  
Call Selling – National Dests.  
Calls placed to premium cost numbers and destinations  
Data – web/email/etc. sessions

Usage Reporting Delays cause

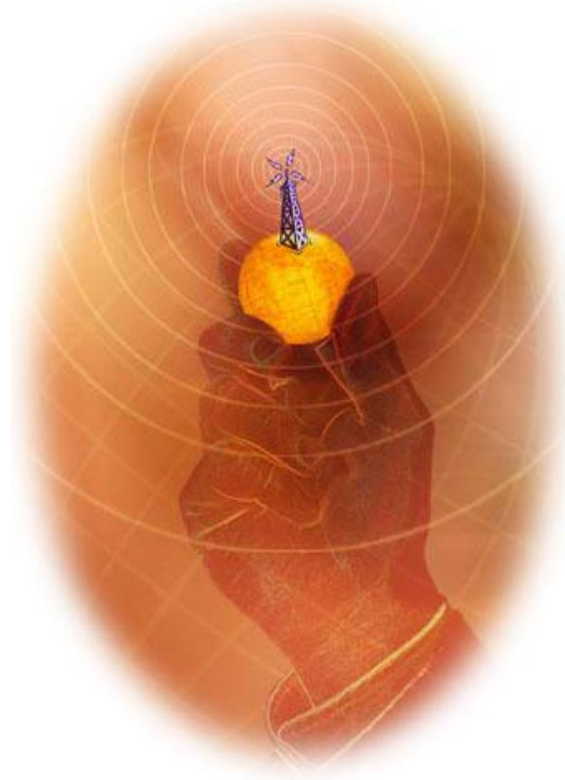
- Delays in fraud detection.
- HUR takes 24 to 36 hours
- Clearinghouses – days (1-7)



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

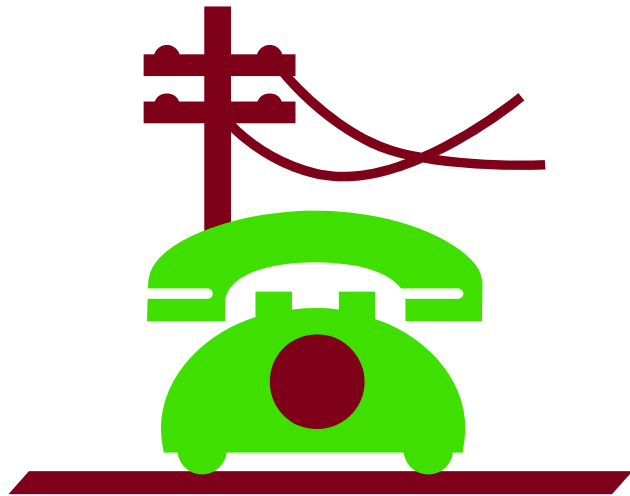
## Bypass Fraud Types

- Wireless (GSM, Amps, CDMA, etc) – use of GSM Gateways is prevalent
- Wire line network Bypass – use of the Internet greatly reduced cost barriers
- Alternate Access Methods – VSAT Satellite systems
- Wireless Border Bleed over – Cross Boundary Wireless Access into other network area



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Terrestrial PSTN Landline Fraud

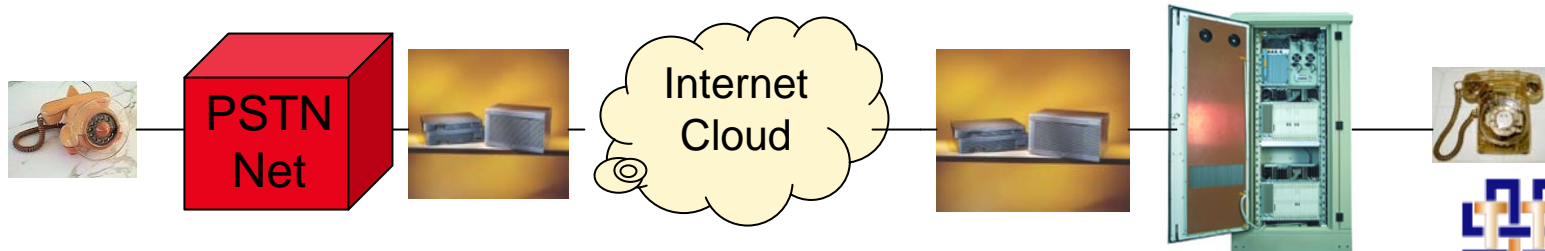


- Bypass Networks Target high international inbound rates
- Bypass Networks Target low local cost areas
- Bypass Networks entire goal is to create arbitrage
- Bypass Networks Target Partners with influence
- Frequent Partners own Hotels, Banks and other high volume Businesses
- Bypass operates where there tends to be a high density of telephone lines



# Terrestrial PSTN Landline Fraud

- Bypass Networks usually never access the International Tandem, other than in cases of insider arrangements.
- Bypass Networks interface transport via Satellite or VoIP networks
- Bypass Networks can use either analog lines (less likely to be discovered) or high capacity lines (E-1 or DS-1)
- Bypass Networks sometimes use CLI stuffers, that delete the original number and stuff a CLI that is appropriate for the termination Route.
- Bypass Networks are usually grouped in batches of 30 lines if digital
- Bypass Networks are usually grouped in batches of 6 if analog

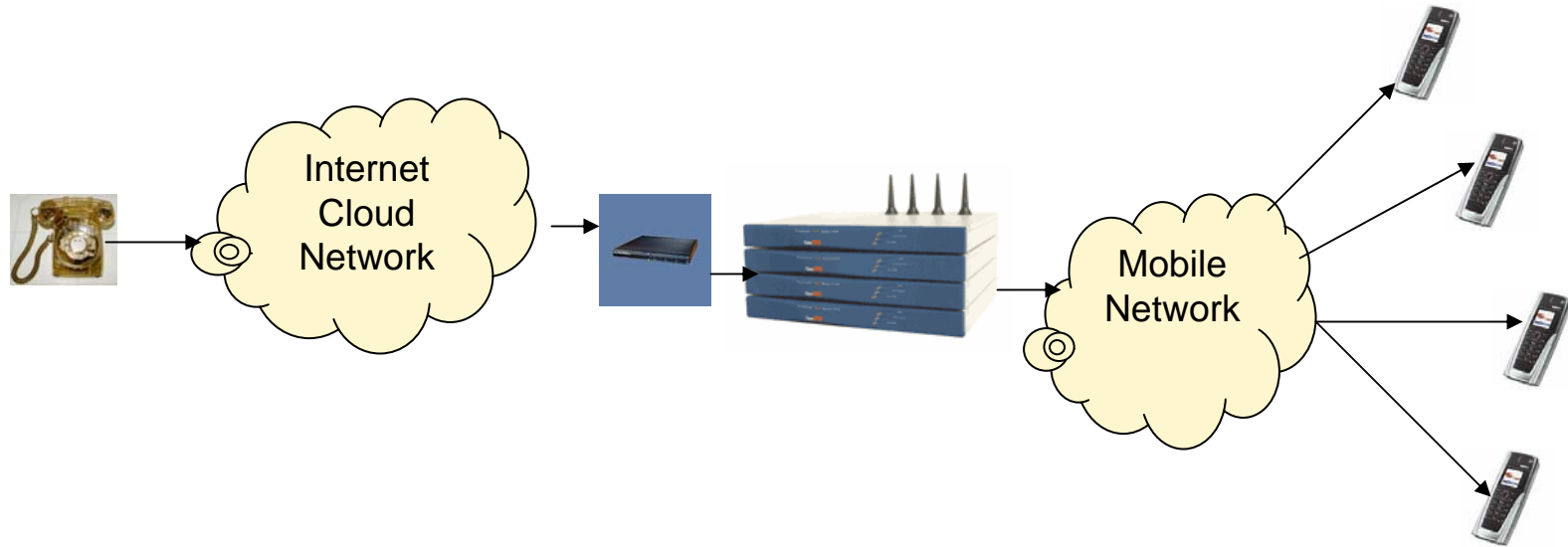


## Typical GSM Bypass Fraud Example

- Call originates in Phoenix, Arizona
- Originating Number is 1.602.470.4065 (Teralight's Phoenix Office)
- The call is placed to a Mobile phone at 92.300.552.1806 in Islamabad
- The call is received on the Mobile phone in Islamabad.
- The CLI on the mobile phone for originating number is ***03XXXXXX1303***. This is not the office number in Phoenix, AZ.
- The call is international, yet it shows a local number.
- A local # is sending the call to mobile phone. **Bypass call!!!**



## Typical GSM Bypass Access Fraud



**GSM Bypass** is very popular for it is very hard to locate the actual Network Bypass link with the origination country or market. Equipment is protected better and the main risk is the actual mobile Number lines when caught, if the ownership of lines is anonymous.



# List of GSM Gateway Manufacturers

## FEATURES

- GSM chip based
- Multiple lines
- Small easy to hide
- Low Power
- Flexible Configurations
- Easy pull out GSM chips
- Good access to programs
- Multiple Sizes and Shapes

2 N

Flosys

Hypermedia Systems

Motorola

Nokia

Quescom

Tellular

Topex

Valiant



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## List of Typical VoIP Manufacturers

### FEATURES

- Small Packaging
- SIP or H.323. v2 compliant
- Multiple Ethernet Ports
- Completely User Configurable
- Secure Log Ins
- Dial Up or Ethernet Backdoor
- Gateway / Gatekeeper CAP
- Generate CDRs Real time
- Improved Algorithms
- Nearly Plug and Play
- Many others

CISCO

Cirillium

Quintum

Vocaltec

Nuera

ECI

Rad

Others



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## List of Typical GSM Quality Issues

- Cost of Bypass Equipment is Higher than other methods
- Greatly increases PDD of telephone Calls
- Introduces additional element of equipment troubleshooting
- Introduces additional programming requirements for far end sites



# GSM Cut-through Improvements



- Dialing Strings are manipulated to request far end to begin cut through of digits, so the systems do not time out and that users do not experience huge post dial delay issues.
- Many GSM systems do not permit cut through, instead opting for store and forward schemes, thereby causing immense post dial delay for all GSM chip Bypass calls.
- Drawing to the left is courtesy of 2N



## Typical Issues Facing Bypass

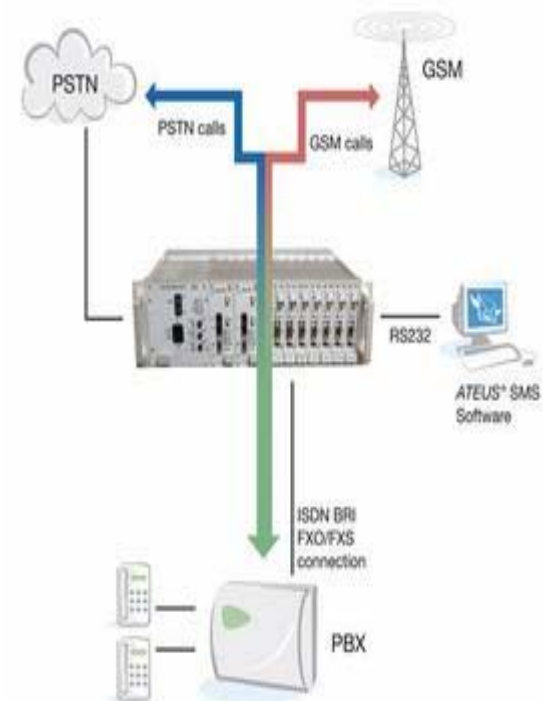


- Highly Illegal in Many countries.
- Revenue is either great or zero
- Highly Risky Operations
- Quality of Routes usually not as good as typical Settlement routes
- Signaling supervision very simple
- SS7 is very difficult to implement
- Billing is suspect, due to non-traditional hard answer supervision
- Equipment lack of expertise locally



## How Bypass Services Work

- New VoIP Technologies permit one end of call to be customer gateway
- Simplicity of network management allows for low barrier to entry
- Partners on Terminating End gain access to local mobile or PSTN
- They use either standard hi-cap or analog PSTN lines, or purchase GSM chips from local mobile supplier
- Generally, VoIP protocol is used, due to very cheap Internet Bandwidth.
- Bypass is usually charged by Week, with LOCs or Cash Deposits
- Many Sites use MMDS or LMDS to “disguise” site locations



## What can Teralight do to Eliminate Fraud?

- Training of what Bypass is. One can't fix a problem if they do not recognize it!
- Design a strategy with the Client, toward Teralight's modular program, that fits the client's needs, budgets and requirements.
- The Physical assignment of Fraud Detection collection abilities is often enough to eliminate a majority of network leakage and Bypass fraud.
- Work closely with Client with regard to the network, SS7 and Billing programs that are currently in place. Engineer the appropriate needs for the Client.
- Implement any necessary Billing System Programming that will allow for automated CDR/IPDR capture, matching and analysis.
- Potentially review entirely the SS7 network of the Client, in order to best engineer the most appropriate methods to collect and analyze Bypass fraud and network leakage.



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## What can Operators do to help Teralight?

- Provide the ability to collect CLI and ANI data as near real time as possible
- Provide an overall synopsis of the network, its associated billing system(s), SS7 utilization and management systems. SS7 is by far the best data collection method available.
- Provide a focus person, by which can work jointly with all parties involved.
- Provide a terminal point on the station side of the network, which enables Teralight to collect real time calls and thus, generate real time CDRs for calls on a test basis.
- Provide Teralight the ability to prove there are illegal access routes, bleeding hundreds of thousands of US dollars per month from revenue streams.



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Methods to Detect Bypass Fraud

- Automatic Systems

Billing systems, SS7 Call Management Systems, others

- Manual Systems

Voice Path Detectors, Call Generators, Line Usage analysis

- Control of both sides of the call

### THE ONLY SURE WAY TO DETECT LEAKAGE REAL TIME

- Teralight will generate calls, manually and automatically from many points of the globe. Such calls will be terminated into special terminal points, that will collect CLI data on the calls. Teralight has offices in Europe, Asia and in North America, all destinations which connect gray routes to originators.



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Automatic Methods to Detect Fraud

- Billing Systems with built in Intelligence to Detect Abnormal use of network
- Billing Systems that generate REAL TIME CDR data (Orcawave, etc)
- Interconnect Billing Systems which are specifically designed for carriers
- Billing Systems that are programmable for customized database management
- Alarm Systems that are user definable and can address multiple channels
- SS7 Networks that are leading edge and utilize ISUP/TUP data management
- SS7 Billing Data for both the Access and the Egress sides of the Calls.
- SS7 Probe Network capabilities (OSIX) that permit data mining
- High Usage Reports that are Real Time and are tied to Alarms



## High Usage Reports



- HUR (High Usage Reports) are a methodology to detect and control Bypass Fraud.
- These reports can be run on a daily basis, but are not usually real time data.
- The levels for which the HUR are set, are Client defined
- The levels are dependent upon the type of business who leases the lines
- High Usage Reports can also be built to look for specific calling patterns



## SS7 Network CLI Management

- SS7 Links provide near real time network analysis
- The CDR/IPDR data collected from the links provides Revenue Assurance systems with more detailed information than the traditional CDRs, thus enabling carriers/ISPs to identify revenue leakage.
- Xsense (Osix) is a carrier class platform for real-time CDR-/IPDR-generation and signaling network surveillance. With Xsense, carriers can increase their revenues, reduce their income shortfall and improve their Quality of Service, which gives a short pay-back time.
- The Xsense probes monitor the traffic in the networks, process and deliver the data to applications downstream. Receivers of this data are Xsense's applications for surveillance for Network Leakage Fraud or the Xsense CDR-/IPDR-generator, which is the interface to third party systems.



## Successful Manual Detect Methods

- Control both sides of the call. Install elements either human resources and or automated dialers to identify source of the call. Design calls to be collected at a specific point of reference in the network. Such calls are already known to be international in nature, whereby any inappropriate local CLI data will be incriminating toward any Bypass operator.
- Build Reference Points in the Network, whereby collected data, when it is a positive match against the database (specific calling trends, etc.), the number, (CDR, IPDR) is then stored in an active database file for further analysis.
- Voice Frequency checks on Data calls – progressive analysis
- Develop CDR Management Systems in Billing Systems which permit immediate ability to ID certain call types and trends.
- There are many tactics which can be used for ID of Fraud.



# Policy Decisions that Eliminate Fraud

Review all High capacity digital line orders

Set up procedures for any order of seven or more analog lines at a time for any small business.

Perform Studies on typical traffic loads for certain Business types

Standardize acceptable amount of traffic on a per line basis for the number of lines ordered for each customer

Insist CLI is available on international tandems and central offices

Create legal standards that are bad for health of Bypass Operators



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Why Teralight Ltd.?

- Hundreds of man years of experience!
- Has built hundreds of routes!
- Understands the international market!
- Clearly has access to Information!
- Ability to serve Pakistan in Pakistan NOW!
- Can test 24 by 7 for Bypass routes!
- Guardian will work with any Billing System!
- We know how to get results from SS7!
- Teralight has people in four continents!
- We are an engineering company. We know Networks!!!



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"

## Teralight, Ltd. Summary

- The ultimate goal of Teralight, Ltd. is to provide the markets in North Africa, Middle East and in South Asia and their respective customers and clients the very best of products and services.
- In order realize to this goal, the company will utilize its diversified resources, including its own consultant base of experience, and professional and business associates, VARs and corporate partners.
- The firm has a large depth of experience in both the enterprise and carrier communications business environments which enables it to pass on to clients and customers valued advice, expertise, and assistance.
- Teralight, Ltd.'s main strength lies in its ability to quickly identify the opportunities available through these vast resources and the unique ability to understand how these opportunities interrelate, and more importantly, how they can be combined to achieve an optimum solution for the client.



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"



Questions???



**TERALIGHT, LTD.**  
"UNITING THE OLD WORLD WITH THE NEW"