

# Telco Fraud Officer

## KUALA LUMPUR 2010

### Week 1: 20-24 September 2010

#### **TFO101: Fraud, Audit and Governance: The Fraud Management Life Cycle**

*Learn from this comprehensive review of the end to end disciplines, tools, methodologies and approaches required to manage a telco Fraud Office.*

#### **TFO102: Network Fraud Primer**

*Learn the basics of the Telecoms Network and where the greatest network fraud and revenue risks can be found.*

#### **TFO103: Interconnect, Bypass and SIMbox Fraud**

*Gain an in-depth analysis of Interconnect and SIMBOX fraud. Learn methodologies for deterrence, detection and diagnosis.*

#### **TFO104: Content/Prepaid Fraud and Fraud-Proofing New Products**

*Learn how to prevent fraudsters from hacking/exploiting new products and systems. Prevent Content and Prepaid frauds.*

#### **TFO105: Roaming Fraud**

*Learn about the fraud-specific difficulties for Prepaid Roaming and Convergent Billing and how to prevent frauds in postpaid and convergent billing.*



### Week 2: 27 Sept - 1 Oct 2010

#### **TFO201: Executive Briefing for Telco Fraud Officers**

*Discover this new, comprehensive and highly effective approach to the containment of Telco Fraud Risk.*

#### **TFO202: Broken Trusts: Accounting, Customer and Employee Fraud**

*Learn about the major categories of accounting, customer and employee fraud. Learn how to deter, detect and pursue frauds in these sensitive areas.*

#### **TFO203: Forensics, Data Warehousing and Law Enforcement**

*Learn Telco Fraud Forensics and Warehousing methods. Learn how to work with internal and external agencies to combat fraud threats.*

#### **TFO204: Techno Fraud, Cyber Crime and Phantom Freaks**

*Learn about the many different technical vulnerabilities that telcos must face, and the different ways to secure them.*

#### **TFO205: 3G Fraud and Money Laundering**

*Learn how to handle the fraud risks that come with new technologies like 3G, GPRS and M-Banking. Be able to protect your telco from fraudsters preying on the vulnerabilities that come with new systems.*

### 1-Day Telco Fraud Crash Courses

#### **TFO410: Executive Overview of Telco Fraud Officer** 27 September 2010

*Gain an overview of the new, comprehensive and highly effective approach to the containment of Telco Fraud Risk, Detection and Deterrence.*

#### **TFO411: Telco Accounting Fraud** 28 September 2010

*Learn about the major categories of accounting fraud, and how to detect and prevent these frauds.*

### 2-Day Telco Fraud Masterclasses

#### **TFO420: Interconnect/Bypass/SIMbox Fraud** 21-22 September 2010

*Gain an in-depth analysis of Interconnect and SIMBOX fraud, as well as detection, deterrence and diagnosis.*

#### **TFO421: Roaming Fraud** 23-24 September 2010

*Learn Telco Fraud Forensics and Warehousing methods. Learn how to work with internal and external agencies to combat fraud threats.*

#### **TFO422: 3G, IP and GPRS Fraud /Money Laundering** 30 Sept - 1 Oct 2010

*Learn how to handle frauds in new lines of business, as well as how these new systems work and how they can be "fraud-proofed."*

Find out more or register for this event:



Certification Information .....3

## Courses Offered at this Event:

### Week 1:

- TFO101 - Fraud, Audit and Governance: The Fraud Management Life Cycle .....4
- TFO102 - Network Fraud Primer .....5
- TFO103 - Interconnect, Bypass and SIMbox Fraud .....6
- TFO104 - Content/Prepaid Fraud and Fraud Proofing New Products .....7
- TFO105 - Postpaid/Convergent Billing Fraud .....8

### Week 2:

- TFO201 - Executive Briefing for Telco Fraud Officers.....9
- TFO202 - Broken Trusts: Accounting, Customer and Employee Fraud.....10
- TFO203 - Forensics, Data Warehousing and Law Enforcement.....11
- TFO204 - Techno Fraud, Cyber Crime and Phantom Phreaks: High Tech Fraud for the High Tech Telecom.....12
- TFO205 - 3G Fraud and Money Laundering.....13

### 1-Day Telco Fraud Crash Courses

- TFO410 - Executive Briefing for Telco Fraud Officers.....14
- TFO411 - Telco Accounting Fraud .....15

### 2-Day Telco Fraud Master Classes

- TFO420 - Interconnect/Bypass/SIMbox Fraud .....16
- TFO421 - Roaming Fraud .....17
- TFO422 - 3G Fraud and Money Laundering .....18

The Revenue Assurance Academy Experience.....19

Contact Us / Event Schedule.....20



## Telco Fraud Certification Credit:

Any student who attends one or more of GRAPA's Telco Fraud Officer Crash Courses or Masterclasses will be eligible for certification credit. Students attending these 1-2 day courses will receive Certificates of Participation that demonstrate what certification curriculum was covered. In order to achieve certification as a Telco Fraud Analyst (I or II), 40 hours of training must be completed, in addition to completion of testing and work verification. Certification as a Master Telco Fraud Officer requires 80 hours of training, in addition to testing and work verification.

---

### Certified Telco Fraud Analyst (I):

The Telco Fraud Analyst (I) Certification provides a detailed understanding of the telecoms revenue chain, as well as clear knowledge of where points of fault, failure or fraud tend to be. Detailed knowledge of how to handle revenue risk provides a crucial grounding in telecoms systems and processes and is essential for fraud professionals to effectively understand where, how and why fraud can be so prevalent in the telecoms context.

---

### Certified Telco Fraud Analyst (II):

The Telco Fraud Analyst (II) Certification focuses on a practical, hands-on, standards-based approach to fraud detection and deterrence. For professionals and practitioners whose daily task is to pursue fraud throughout their organization, this is an essential program of training and credentialization. It provides the key tools, techniques, methods and structures necessary for fraud analysts to prioritize their case load, understand what the largest and most dangerous fraud are, as well as how to identify fraudsters and build cases for successful prosecution.

---

### Certified Master Telco Fraud Officer :

The Certified Master - Telecoms Fraud Officer reports to top management (usually directly to the CEO) regarding the entirety of fraud exposures for the telco. The Telecoms Fraud Officer directs a team of Telecoms Fraud Analysts, orchestrating cooperation with legal, regulatory, security, fraud management, revenue assurance and internal audit to ensure the entirety of a telco's fraud exposures are being addressed and controlled. GRAPA's certification provides professionals with the tools, techniques and methods to effectively detect and deter fraud across all telco domains.



Learn about the GRAPA Fraud Deterrence and Detection Lifecycle, a comprehensive review of the end to end disciplines, tools, methodologies and approaches required to manage a telco Fraud Office.

## Overview

Telecommunications companies today are focused on the development and deployment of radical new technologies and business models—technologies that are reshaping how the world communicates, shares and works—but too many fraud managers spend their time looking backwards, trying to figure out how to over-secure areas and products that are not in danger, while ignoring the areas that are a major fraud risk.

Discover how GRAPA is helping turn Telco Fraud Detection and Deterrence into one of the most effective functions within the modern Telco by providing fraud managers with perspectives and techniques that get them focused on securing the areas that are most vulnerable and susceptible to fraudsters' schemes - allowing them to offer significant and immediate value to their organization.

**Duration:** 1 Day

## Who Should Attend?

Experienced Telecoms Fraud Management personnel, as well as those new to the industry and field, who are interested in the functions of a Telco Fraud Office, and want to learn the required disciplines, tools, methodologies and approaches.



## Fraud, Audit and Governance: The Fraud Management Life Cycle

### Curriculum Outline

The Real Telco Operations Model

The Role of Fraud Deterrence and Detection in the Integrated Revenue Governance Framework

GRAPA's Fraud Deterrence and Detection Lifecycle

GRAPA Fraud Standards, Policies and Guidelines

Revenue Mapping and Fraud KPIs and Management

## Key Concepts include:

- ▶ The Fraud Deterrence and Detection Lifecycle
- ▶ Forensics, Risk Analysis
- ▶ 12 types of fraud controls and how to apply them
- ▶ Definition of the Role of Fraud Management
- ▶ Principles of KPI Design and Deployment
- ▶ Case Management
- ▶ Incident Management
- ▶ Process of Elimination
- ▶ MOU Analysis
- ▶ Exploit Libraries
- ▶ GRAPA Standard Controls
- ▶ Telco Fraud Body of Knowledge
- ▶ Telco Fraud Officer Standards
- ▶ GRAPA Certification Programs
- ▶ Revenue Mapping

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- The Real TOM
- The Science of Fraud management
- The Fraud Deterrence and Detection Lifecycle
- Fraud Standards and Procedures
- Principles of Incident Management
- Principles of Case Management
- Revenue Mapping
- Integrated Revenue Governance and Management

Network basics for the technically challenged. The training provided will turn normal people into experts in all aspects of network fraud

## Overview

Network jargon and concepts simplified and demystified so that anyone can understand them.

You cannot claim to understand Telco fraud deterrence and detection without understanding the underlying network!

All of the terms, concepts and "tricks of the trade" that make it possible for you to understand, review and question the network side of the fraud management equation. Students in this course will learn the key fundamentals to protect telecom systems and revenues. This course will also cover the basics of mediation and postpaid billing systems, which is crucial being able to effectively deter and detect frauds in these areas.

**The material covered during this course is a prerequisite for most advanced fraud management issues.**

**Duration:** 1 day

## Who Should Attend?

Experienced Telco Fraud Professionals as well as those new to the industry and field who are looking to better understand the complex network they are protecting



## Network Fraud Primer

### Curriculum Outline

Network Foundations for Fraud Management
CDR Processing Principles (Mediation, Postpaid)
Fraud Management Systems Operation
CDR - AAA (Authentication, Authorization, Accounting)
Network Security/ Fraud Protection

## Key Concepts include:

- ▶ Principles of circuit technology
- ▶ Key network controls and methods
  - Topology, Security, Control Protocol, Transaction Control,
  - CDR Generation Sequence, CDR Generation, CDR Transport
- ▶ Media characteristics and controls (*wireless and wireline*)
- ▶ History of Circuit Technology
- ▶ Understanding SS7
- ▶ Mediation Operations
  - ▶ Mediation Fraud Management
- ▶ Postpaid Billing Operations
  - ▶ Postpaid Billing Fraud Management
- ▶ Fundamentals of Fraud Management Systems
- ▶ Advanced Fraud Management System Administration
- ▶ AAA (Authentication, Authorization, Accounting) for Network
- ▶ Network Fraud Controls and Methods

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- Principles of Network Operations and Management
- Wireless and Wireline Media Characteristics
- Billing Architectures and Controls
- Control Protocols Principles and Applications
- SS7 Principles
- Fraud Management System Fundamentals
- Advanced Fraud Management Systems
- Network Security and Fraud Protection
- CORE AAA
- Principles of Mediation Operations
- Principles of Post Paid Billing Operations
- Postpaid and Mediation Fraud Exploits and Remedies

This course was designed to provide students with an in-depth analysis of Interconnect and SIMBOX fraud. Fraud professionals will learn methodologies for deterrence, detection and diagnosis.

## Overview

This course was designed to provide students with an in-depth analysis of Interconnect and SIMBOX fraud. Fraud professionals will learn methodologies for deterrence, detection and diagnosis.

After this class, students will be able to:

- Define the principle fraud vulnerabilities of a telco in the areas of International and domestic interconnect
- Understand the architecture, market, regulatory and fraud issues associated with international and domestic interconnect
- Understand bypass fraud in the areas of interconnect partner/competitor illegal bypass, SIMBOX bypass, VOIP / Internet bypass
- Detect, deter, prosecute and protect the telco from these vulnerabilities
- Understand the role of third party bypass detection providers, what they do, and how they deliver value

**Duration:** 1 Day

## Who Should Attend?

Experienced Telcoms Fraud Management personnel, as well as those who are new to the industry/field, who are interested in gaining an in-depth analysis of the detection, deterrence and diagnosis of Interconnect, Bypass and SIMbox Frauds.



## Interconnect, Bypass and SIMbox Fraud

### Curriculum Outline

Interconnect Operations

Regulators Dilemma - Interconnect Regulation

External/Internal Interconnect Fraud

Denial of Revenue Attacks

Bypass Fraud/SIMbox Fraud

## Key Concepts include:

- ▶ Fundamentals of Interconnect Operations
- ▶ Interconnect Network Design and Constraints
- ▶ Interconnect CDR Topologies and Billing Controls
- ▶ CDR security for interconnect
- ▶ Trunk Group Security and controls
- ▶ Interconnect routing table security, issues and controls
- ▶ Settlement process operations
- ▶ Settlement fraud risks and controls
- ▶ Internal Interconnect Frauds and their Prevention
- ▶ External Interconnect Frauds and Their Prevention
- ▶ Denial of Revenue Attacks
- ▶ Fundamentals of BYPASS Fraud
- ▶ Fundamentals of SIMBOX Operations
- ▶ Bypass Mapping and Assessment Approach
- ▶ Working with Law enforcement and regulators
- ▶ Working with Third Parties to combat Interconnect Fraud

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- Principles of Interconnect Operations (Functions, Forensics and Controls)
- LOB Principles Interconnect
- External and Internal Interconnect Frauds
- Denial of Revenue Attacks
- Principles of SIMBOX operation, detection and deterrence
- Principles of BYPASS operation, detection and deterrence

## Protect New Products From Fraud, Fraud-Proof Content and Prepaid Billing

New content is being offered, opening new forms of fraud. Protect your Telco from these new frauds and hacks.

### Overview

Telco success depends on the ability to deploy newer and better technologies faster than anyone else. But the pace of deployment creates a fraud management "black hole" that must be addressed.

Learn how to get in front of new technologies before they create fraud problems that cannot be handled. Apply proven methodologies to manage new product development and deployment for maximum impact at minimum cost.

Protect your Telco's Prepaid Billing systems from all forms of fraud.

**Duration:** 1 Day

### Who Should Attend?

Experienced Telecoms Fraud Management personnel and those new to the industry/field who are interested in learning more about protecting new products from fraud schemes, as well as how to protect prepaid and content from fraud hacks.



## Content/Prepaid Fraud and Fraud-Proofing New Products

### Curriculum Outline

SMS, MMS, WAP, Content Operations and Fraud Management

New Product Development and the role of Fraud Management

Prepaid Control Domains and Fraud Management (Traffic, Channel, Rating, Account)

Prepaid Fraud Controls

### Key Concepts include:

- ▶ Fundamentals of Operations and Fraud Controls for:
  - ▶ SMS
  - ▶ MMS
  - ▶ WAP
  - ▶ Content
- ▶ Fundamentals of New Product Development in Telecom
- ▶ Role of Fraud Mgmt in the security of new products/services
- ▶ Prepaid Operations and Fraud Vulnerabilities
- ▶ Traffic Frauds and Hacks
  - ▶ Channel Frauds
  - ▶ Top Up Theft / Cons
  - ▶ Printer Cons
  - ▶ IN Hacks
  - ▶ Securing Requisitioning Channels
  - ▶ Securing Logistics and Sales Channels
  - ▶ Dealer Frauds
  - ▶ Sales Frauds
  - ▶ Rating Process and Rate Frauds
  - ▶ Account Management Containment
  - ▶ Customer Service Frauds
  - ▶ Accounting Frauds
  - ▶ Programmer / contractor frauds
  - ▶ Fraud controls for accounts

### GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- Product Architectures - SMS, MMS, WAP, Content
- Content Operations (Functions, Forensics and Controls)
- Content Fraud Exploits, Cases and Remedies
- Fundamentals in New Product Development (Fraud and RA)
- Role of Fraud Management in New Product Deployment
- Principles of Prepaid Billing Assurance
- LOB Principles - Prepaid
- Traffic, Channel, Account and rating Assurance Controls and Corrections
- Prepaid Fraud Exploits, Cases and Remedies
- Prepaid Fraud Controls

Learn the Fraud Management-specific difficulties for Prepaid Roaming and Convergent Billing, as well as the basic functions of a Convergent Billing System, CAMEL System and more.

## Overview

Camel and Roaming Fraud represent one of the single largest sources of losses for telecoms around the world today. This course will teach you how to detect and prevent fraud losses from internal fraudsters, roaming partners, DCH's and professional fraud makers.

**Duration:** 1 Day

## Who Should Attend?

Experienced Telecoms Fraud Management personnel as well as those new to the industry and/or field who are interested in learning the details of Postpaid and Convergent Billing Fraud risks.



## Roaming/Convergent Billing Fraud

### Curriculum Outline

Postpaid Roaming Operations and Fraud Controls

USSD Roaming Operations and Fraud Controls

Prepaid Roaming - Operations and Fraud Controls

Convergent Billing - Operations

Credit Frauds

## Key Concepts include:

- ▶ Postpaid Roaming Methods and Procedures
- ▶ HUR and NRTDE Roaming Credit Management
- ▶ Roaming SS7 Topology and Architecture
- ▶ Protecting against roaming traffic frauds
- ▶ Roaming clone frauds
- ▶ DCH role and frauds
- ▶ USSD Roaming Methods , operations and procedures
- ▶ Securing USSD revenues
- ▶ CAMEL Roaming - Opeations and Controls
- ▶ CAMEL Roaming - principle fraud risks
- ▶ Convergent Billing Systems Architecture
- ▶ Five categories of Convergence:
  - ▶ Billing Singularity
  - ▶ LOB Fusion
  - ▶ Rating Amalgamation
  - ▶ Credit Confluence
  - ▶ Account management unification
- ▶ Key fraud risks and containments in Convergent Billing

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees **Competency Credit** for the following areas in line with GRAPA's "Body of Knowledge"

- Principles of Postpaid Roaming Operations (Functions, Forensics and Controls)
- Principles of USSD Prepaid Roaming (Functions, Forensics and Controls)
- Principles of Prepaid (CAMEL) Roaming (Functions, Forensics and Controls)
- Roaming Fraud Exploits , Cases and Remedies
- Roaming Fraud Management
- Convergent Billing Operations (Functions, Forensics and Controls)
- Convergent Billing Fraud Exploits, Cases and Remedies

Discover this new, comprehensive and highly effective approach to the containment of Telco Fraud Risk, Detection and Deterrence.

## Overview

The need for a significant and immediate improvement in the way that telecoms deter and detect fraud in all of its many different aspects is both obvious and compelling. The staggering losses reported by carriers each year indicate that in many cases some drastic measures are called for to help stem the tide of fraud risk that the typical telco is exposed to.

In this groundbreaking new course, GRAPA provides fraud related professionals with what is probably their first-ever comprehensive end-to-end review and approach to the management of telco fraud exposures throughout the Telco.

In this one-day class we will introduce the student to the foundational concepts and facts related to the full range of fraud exposures that the typical telco faces, and present a standardized, systematic, comprehensive and effective approach for the containment, detection and deterrence of those risks.

**Duration:** 1 Day

## Who Should Attend?

Experienced Telecom Fraud Management personnel (especially executives, C-Levels and Directors) as well as those new to the industry and field who are interested in finding out more about GRAPA's effective approach to the containment of Telco Fraud Risk, Detection and Deterrence.



## Executive Briefing for Telco Fraud Officers

### Curriculum Outline

What is Fraud

Profiling Techniques (Situational, Behavioral)

Fraudster Profiling

GRAPA - Fraud Lifecycle and Standards

Fraud Exploit Libraries and Circle of Trust

## Key Concepts include:

- ▶ The Telco Fraud Officer Concept,
- ▶ Measuring Telco Fraud and Fraud Risk,
- ▶ Fraud Risk Assessment Methods,
- ▶ The Fraud Detection and Deterrence Lifecycle,
- ▶ Target Decomposition Techniques
- ▶ Method of Ingress Analysis, Exploit Analysis
- ▶ Inventory of Exploits
- ▶ Case Studies in Fraud, Controls, Corrections, Prosecution, Investigative Techniques
- ▶ Fraudster Profiling
- ▶ Roles and Responsibilities of a Telco Fraud Officer
- ▶ Case Management Discipline and Rationalization
- ▶ Incident Triage
- ▶ Forensic Accounting Techniques
- ▶ Forensic Analytics
- ▶ Customer Fraud Exploits
- ▶ Targets
- ▶ MOI and MOA
- ▶ Prosecution Benefits
- ▶ Methods and Issues
- ▶ Prosecution Advocacy
- ▶ Financial Audit Techniques

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- The GRAPA Fraud Tree – Domain Decomposition including Domain Knowledge, Target Decomposition, Diagnosis, Method of Ingress, Exploits, Controls, Corrections, Compliance, Prosecution and Fraudster Profiling
- Network Intrusion Domain Profile
- Supply Chain and Inventory Management Domain Profile
- Revenue Stream Domain Profile
- CRM and Sales Domain Profile
- Partner and Bypass Domain Profile
- Averse Accessory Domain Profile
- Accounting and Administration Domain Profile
- The GRAPA Fraud Detection and Deterrence Lifecycle
- Principles and Methods of Investigation
- Principles and Methods of Case Development and Prosecution Advocacy
- Principles and Methods of Controls Development, Execution and Compliance Reporting
- Telco Fraud Officer Profile – Job Description, roles, responsibilities
- Telco Fraud Officer Interfaces and Models of Cooperation - Interfacing with ternal (audit, revenue assurance, security) and external (law enforcement, regulatory, governmental) agencies and departments

Learn about the major categories of accounting, customer and employee fraud. Learn how to deter, detect and pursue frauds in these sensitive areas.

## Overview

In this class, we will focus on the issues related to the security and integrity of the telco when it comes to accounting, customers and employees.

There are many areas where the telco is especially vulnerable to fraudulent attack. The biggest include: In the sales and customer service areas, wherever inventories, contracts and supply chain management are concerned or with accounting systems and controls. In this class we provide the student with a comprehensive review of each of these areas, and consider the best ways to detect, prevent and prosecute them when they do occur.

The issues of fraud detection, deterrence and prosecution are more sensitive in this area than in any other area. While people will hardly ever resist the thought of prosecuting outright professional criminals, it often gets to be much more difficult to figure out what do to about internal fraud cases. In this course, we will provide students with a set of step-by-step guidelines for the detection, investigation and case management process. Case management with a due sensitivity to the interpersonal, H/R, legal, investor and market issues associated with these kinds of situation.

**Duration:** 1 day

## Who Should Attend?

Experienced Telcoms Fraud Management personnel and those new to the field who are interested in learning more about internal frauds, customer fraud and accounting fraud.



## Broken Trusts: Accounting, Customer and Employee Fraud

### Curriculum Outline

Cash and Expense Fraud Mgmt
Purchasing, Payroll, H/R and Capital Frauds
Accts Payable, Accts Recivable Frauds
Inventory and Logistics Frauds
Customer Frauds and Financial Forensics

## Key Concepts include:

- ▶ The size, extent and nature of customer and employee based fraud
- ▶ The primary domains of customer and employee based fraud including:
  - ▶ CRM
  - ▶ Sales Channel
  - ▶ Supply Chain
  - ▶ Inventory Management
  - ▶ Accounting and Administration Fraud
  - ▶ Key Domain Characteristics
  - ▶ Targets
  - ▶ Methods of Ingress
  - ▶ Principle Exploits
- ▶ Methods for detection of fraud in each of these cases
- ▶ Forensic Accounting techniques
- ▶ Accounting Fraud Evidence Gathering

## GRAPA Fraud Officer Certification Credit

Successful completion of this course, testing and experience verification will result in the student being awarded GRAPA Fraud Officer Competency Credit for the following areas from the GRAPA Fraud Officer "Body of Knowledge":

- CRM and Sales Fraud Domain Analysis and Method of Address (MOA)
- Supply Chain and Inventory Mgmt Fraud Domain Analysis and MOA
- Accounting and Administration Fraud Domain Analysis and MOA
- Financial Audit Techniques, Methods and Objectives
- Sales Channel Exploits (Methods of Intrusion, Target Domains, Cases)
- Inventory and Supply Chain Exploits (Methods of Intrusion, Target Domains, Cases)
- Accounting Fraud Exploits (Methods of Intrusion, Target Domains, Cases)
- Investigative procedures and techniques
- Case management: Building Cases and Advocacy for Case prosecution
- Prosecution: Methods, Issues and Benefits
- Case Dispensation and Resolution
- Customer Fraud Exploits (Methods of Intrusion, Target Domains and Case Management)
- Case Development Workshop

Learn how to organize and optimize your Fraud Officer operations. Gain knowledge on how to profile professional criminals, terrorists and other people with professional intent to do harm, and learn how to work with internal and external agencies to combat these threats.



## Overview

The telecommunications company represents the single most powerful and pervasive form of communication known to man, and the creative energies of criminals and terrorists are constantly being applied in order to determine new ways to leverage this power to their advantage.

Students in this class will learn the methodology and best practices for fraud management, forensics and data warehousing and data mining for telecoms fraud. Students will learn to use data warehousing, or a "forensics lab," to maintain a database of fraudster schemes for use in future investigations. Data mining techniques will be covered to ensure students are capable of locating key characteristics of a typical fraudster and using this knowledge to their advantage to enhance investigations.

In this class we focus on the professional criminal and a special domain of fraud known as Averse Accessory Fraud. Under the Averse Accessory scenario, criminals and terrorists make use of the telecommunications company's assets in order to cheat others. The telco is an unwilling participant in the fraud (an averse accessory), but the telco will still often suffer legal, ethical and criminal liability if due diligence is not maintained.

Working with regulators, government and law enforcement has always been a critical aspect of the role of the telecom, and the fraud officer is a key part of that process.

**Duration:** 1 Day

## Who Should Attend?

Experienced Telecoms Fraud Management personnel as well as those new to the field who are interested in learning more about working with Law Enforcement, as well as forensics and data warehousing for fraud management.

## Forensics, Data Warehousing and Law Enforcement

### Curriculum Outline

Managing Fraud Operations - Establishing TFO
Forensics: Data Warehousing and Data Mining for Fraud
Legal and Logical Forensics
Law Enforcement and Government activities
Averse Accessory and CPE Frauds

## Key Concepts include:

- ▶ Data Warehousing and Building the Fraud Forensics Laboratory
- ▶ Data Mining for Fraud Forensics
- ▶ Working with Law Enforcement
- ▶ Government Responsibilities
- ▶ Legal Intercept Systems
- ▶ Traffic monitoring and disclosure laws and requirements
- ▶ Anti-Terrorism activities and controls
- ▶ Averse accessory Frauds
- ▶ Key concepts in LEGAL FORENSICS and Legal Logic
- ▶ Logical Forensics Methods
- ▶ Coyote Management Disciplines
- ▶ Management in the 21st Century

## GRAPA Fraud Officer Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- Averse Accessory Fraud Domain Analysis and MOA (Method of Address)
- Law Enforcement Evidentiary Techniques
- Fundamentals of Law and Jurisdiction applied to telecoms
- CALEA (the US Law Enforcement Standards) as applied to Telecoms
- Working with external organizations in order to combat fraud of all types
- Electronic surveillance, bugs, wiretaps, radio intercept, GPS – Location tracking and other legally constrained activities
- Bribery, Extortion, Con Games, Identity Theft and other forms of averse accessory fraud and telecom liabilities
- Coyote Management and 21st century management principles
- Data Warehousing for Fraud Forensics
- Data mining for Fraud Forensics
- Legal Forensics - Principles and Application
- Logical Forensics - Principles and Application

Telecommunications is a high tech business, so it should come as no surprise that it is in the technology area where many telcos are hit the hardest. In this class we review the far reaching and technically sophisticated world of techno fraud.

## Overview

The telco is a high technology engine, racing to provide the latest services and technologies to consumers at an ever-accelerating pace. However, this race to market brings with it a significant amount of risk when it comes to fraud. While telcos are undeniably the launching pad for these many different technologies, they are equally responsible for the fraudulent exposures that these innovations generate.

This class takes the student on a focused, detailed and eye opening journey into the diverse range of technologies and vulnerabilities associated with the deliverance of “bleeding edge technology” to the public.

In this class you will learn about each of these areas, how they are being exploited by fraudsters, criminals and terrorists, and how they can be better understood and protected.

**Duration:** 1 day

## Who Should Attend?

Experienced Telcoms Fraud Management personnel as well as those who are new to the field of fraud management who are interested in learning about the fraud risks involved in launching new technologies



## Techno Fraud, Cyber Crime and Phantom Phreaks

### Curriculum Outline

Network Frauds and Methods of Access
Hacks, Phreaks and Attacks
Core Telecoms Network
Web-based Hacking
Attacks and Methods of Access (MOA)
LAN-Based Wireless Network

## Key Concepts include:

- ▶ The Principle Domains, Exploits and Characteristics of Techno-Fraud
- ▶ Cyber-Terrorism and Phreaking
- ▶ Authentication, Authorization, Accounting
- ▶ Reference File Protection, Transaction File Protection
- ▶ Network Topology
- ▶ Major Techno-Exploits and Methods of Intrusion
- ▶ Hacking
- ▶ Credential Falsification
- ▶ Identity Falsification
- ▶ Types of Hacks, including SMSC Hacks, Firewall Hacks, Gateway Hacks, Portal Hacks, WAP Server Hacks, Content Server Hacks, Radius Server Hacks, Customer Premise Equipment Hacks, IP-PBX Hacks, Email Server Hacks, VMail Server Hacks
- ▶ Bugging
- ▶ Radio Intercept
- ▶ GPS Intercept
- ▶ Blackmail and Extortion
- ▶ Ethical Hacking
- ▶ Telecoms Core Network Hacks, Vulnerabilities and Case Studies
- ▶ Wireless (GSM/CDMA/3G) Hacks, Vulnerabilities, Phreaks and Cases
- ▶ LAN Management, Controls and Hacks
- ▶ Web and Internet vulnerabilities, methods

## GRAPA Fraud Officer Certification Credit

Successful completion of this course, testing and experience verification will result in the student being awarded GRAPA Fraud Officer Competency Credit for the following areas from the GRAPA Fraud Officer "Body of Knowledge":

- Network Intrusion Fraud Domain and Method of Address (MOA)
- Physical Network Security/Violation – Domains, Exploits, MOA
- Logical Network Security/Violation – Domains, Exploits, MOA
- Hacking – Techniques, MOA
- Phreaking – Techniques, MOA
- Customer Premise Equipment Violation – Domains, Exploits, MOA
- Logical Lease Domain Violation – Domains, Exploits, MOA
- Domain Review – Circuit Components: IN, MMSC, SMSC, WAP Server
- Domain Review – Packet Components: Email Server, Web Server, Content Server, Firewalls, Portals, Gateways, Radius Servers
- Domain Review – Radio Components: RNC, Node B, BTS, BSC

Learn how to handle the fraud risks that come with new technologies such as Internet, 3G, GPRS and M-Banking. Be able to protect your telco from fraudsters preying on the vulnerabilities that come with these new systems.

## Overview

Key areas covered during this course include fundamentals of network topology design and security issues, key operational principles of packet technology, the SIP and VOIP protocols and operational architectures and Packet-Based billing models and their assurance/fraud proofing.

After covering these core technology issues, students will be provided with an in-depth consideration of the architecture, operational models, billing models and fraud risks associated with GPRS and "wireless internet," Core wireline based internet (DSL/Cable/WIMAX) and 3G, Next generation network (NGN) and Media Gateway Frauds and Exposures.

In addition, students will learn about the major issues associated with Money Laundering that is plaguing telecoms around the world, the relationship of the telco to the banking regulatory agencies, and the architecture, issues and deployment of M-Banking systems.

**Duration:** 1 day

## Who Should Attend?

Experienced Telcoms Fraud Management personnel and those new to the industry and field who want to learn more about fraud risks associated with new technologies like 3G, GPRS and more.



## Forensics, Data Warehousing and Law Enforcement

### Curriculum Outline

Packet-Based Topologies and Architectures
SIP/VOIP and Packet-Based billing challenges
GPRS Operations, Billing and Frauds
3G, Internet and IP Frauds
Money Laundering for Telcos
Mobile Banking Systems and Fraud Protection

## Key Concepts include:

- ▶ Network Topology
- ▶ Network Security
- ▶ Principles of packet based technology
- ▶ ATM vs IP
- ▶ IP Protocol Family
- ▶ SS7 Review
- ▶ SIP and SS7 Relationship
- ▶ VOIP alternative business and billing models
- ▶ GPRS Architecture
- ▶ SGSN/GGSN Functions and Architectures
- ▶ APN Protection and APN Hacks
- ▶ PDP assignment and security
- ▶ Alternative GSN billing models
- ▶ Prepaid SGSN connections
- ▶ GRAPA standard GPRS controls and assurance
- ▶ 3G Technologies
- ▶ LTE vs UMTS vs IETF Frameworks
- ▶ Assuring and Security MGW and NGN
- ▶ Money Laundering and Banking Regulations
- ▶ Mbanking Architectures and Security

## GRAPA Fraud Officer Certification Credit

Successful completion of this course, testing and experience verification will result in the student being awarded GRAPA Fraud Officer Competency Credit for the following areas from the GRAPA Fraud Officer "Body of Knowledge":

- MBanking
- Money Laundering
- NGN Security
- MGW Security
- GPRS Security
- SIP/VOIP Principles
- Packet Billing Models
- Principles of Packet Based Services and Billing
- SIP/Voip Operations and Principles
- VOIP Billing and Assurance
- Principles of GPRS Operations (Functions, Forensics and Controls)
- GPRS Security and Fraud Management
- Principles of 3G, LTE, UMTS and IMS (Functions, Forensics and Controls)
- 3g, LTE, IMTS and IMS Fraud management

Learn an overview of the new, comprehensive and highly effective approach to the containment of Telco Fraud at this 1-Day Telco Fraud Masterclass.

## Overview

The need for a significant and immediate improvement in the way that telecoms deter and detect fraud in all of its many different aspects is both obvious and compelling. The staggering losses reported by carriers each year indicate that in many cases some drastic measures are called for to help stem the tide of fraud risk that the typical telco is exposed to.

In this 1-Day Masterclass, GRAPA provides fraud related professionals with what is probably their first-ever review and approach to the management of telco fraud exposures throughout the telco. This course provides an executive overview of the functions and principles for the Telco Fraud Officer.

In this one-day class we will introduce the student to the foundational concepts and facts related to the full range of fraud exposures that the typical telco faces, and present a standardized, systematic, comprehensive and effective approach for the containment, detection and deterrence of those risks.

**Duration:** 1 Day

## Who Should Attend?

Experienced Telco Fraud Professionals (especially Executives, C-Levels, Directors) or those new to Telecoms Fraud who are interested in understanding the principles and approaches to Telco Fraud Risk, Detection and Deterrence.



## 1-Day Crash Course: Executive Briefing for Telco Fraud Officers (TFO201)

### Curriculum Outline

What is Fraud
Profiling Techniques (Situational, Behavioral)
Fraudster Profiling
GRAPA Fraud Lifecycle and Standards
Fraud Exploit Libraries and Circle of Trust

### Key Concepts include:

- ▶ The Telco Fraud Officer Concept,
- ▶ Measuring Telco Fraud and Fraud Risk,
- ▶ Fraud Risk Assessment Methods,
- ▶ The Fraud Detection and Deterrence Lifecycle,
- ▶ Target Decomposition Techniques
- ▶ Method of Ingress Analysis, Exploit Analysis
- ▶ Inventory of Exploits
- ▶ Case Studies in Fraud, Controls, Corrections, Prosecution, Investigative Techniques
- ▶ Fraudster Profiling
- ▶ Roles and Responsibilities of a Telco Fraud Officer
- ▶ Case Management Discipline and Rationalization
- ▶ Incident Triage
- ▶ Forensic Accounting Techniques
- ▶ Forensic Analytics
- ▶ Customer Fraud Exploits
- ▶ Targets
- ▶ MOI and MOA
- ▶ Prosecution Benefits
- ▶ Methods and Issues
- ▶ Prosecution Advocacy
- ▶ Financial Audit Techniques

### GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- The GRAPA Fraud Tree – Domain Decomposition including Domain Knowledge, Target Decomposition, Diagnosis, Method of Ingress, Exploits, Controls, Corrections, Compliance, Prosecution and Fraudster Profiling
- Network Intrusion Domain Profile
- Supply Chain and Inventory Management Domain Profile
- Revenue Stream Domain Profile
- CRM and Sales Domain Profile
- Partner and Bypass Domain Profile
- Averse Accessory Domain Profile
- Accounting and Administration Domain Profile
- The GRAPA Fraud Detection and Deterrence Lifecycle
- Principles and Methods of Investigation
- Principles and Methods of Case Development and Prosecution Advocacy
- Principles and Methods of Controls Development, Execution and Compliance Reporting
- Telco Fraud Officer Profile – Job Description, roles, responsibilities
- Telco Fraud Officer Interfaces and Models of Cooperation - Interfacing with ternal (audit, revenue assurance, security) and external (law enforcement, regulatory, governmental) agencies and departments

Learn about the major categories of accounting fraud. Learn how to detect, deter and handle the sensitive issues in this area.

## Overview

In this class, we will focus on the issues related to the security and integrity of the telco when it comes to accounting fraud.

Accounting fraud represents one of the largest and the best understood of the telco fraud domains. Unfortunately, while well understood by accountants in other industries, telco fraud officers often need some basic education in these areas. In this class, we consider the overall category of accounting fraud and the history, role and major components of the accounting process.

This class will provide the student with a comprehensive review of telco accounting fraud risks, principle and how to detect and prevent accounting frauds from occurring.

The issues of fraud detection, deterrence and prosecution are more sensitive in this area than in any other area. While people will hardly ever resist the thought of prosecuting outright professional criminals, it often gets to be much more difficult to figure out what do to about internal fraud cases such as accounting fraud. In this course, we will provide students with a set of step-by-step guidelines for the detection, investigation and case management process.

**Duration:** 1 day

## Who Should Attend?

Telco Fraud Professionals who are interested in the specific risks and vulnerabilities involved in the sensitive area of Accounting Fraud.



## 1-Day Crash Course: Telco Accounting Fraud (TFO202)

### Curriculum Outline

- Cash and Expense Fraud Mgmt
- Purchasing, Payroll, H/R and Capital Frauds
- Accounts Payable, Accts Recivable Frauds
- Inventory and Logistics Frauds
- Customer Frauds and Financial Forensics

### Key Concepts include:

- ▶ The size, extent and nature of customer and employee based fraud
- ▶ The primary domains of customer and employee based fraud including:
  - ▶ CRM
  - ▶ Sales Channel
  - ▶ Supply Chain
  - ▶ Inventory Management
  - ▶ Accounting and Administration Fraud
  - ▶ Key Domain Characteristics
  - ▶ Targets
  - ▶ Methods of Ingress
  - ▶ Principle Exploits
- ▶ Methods for detection of fraud in each of these cases
- ▶ Forensic Accounting techniques
- ▶ Accounting Fraud Evidence Gathering

### GRAPA Fraud Officer Certification Credit

Successful completion of this course, testing and experience verification will result in the student being awarded GRAPA Fraud Officer Competency Credit for the following areas from the GRAPA Fraud Officer "Body of Knowledge":

- CRM and Sales Fraud Domain Analysis and Method of Address (MOA)
- Supply Chain and Inventory Mgmt Fraud Domain Analysis and MOA
- Accounting and Administration Fraud Domain Analysis and MOA
- Financial Audit Techniques, Methods and Objectives
- Sales Channel Exploits (Methods of Intrusion, Target Domains, Cases)
- Inventory and Supply Chain Exploits (Methods of Intrusion, Target Domains, Cases)
- Accounting Fraud Exploits (Methods of Intrusion, Target Domains, Cases)
- Investigative procedures and techniques
- Case management: Building Cases and Advocacy for Case prosecution
- Prosecution: Methods, Issues and Benefits
- Case Dispensation and Resolution
- Customer Fraud Exploits (Methods of Intrusion, Target Domains and Case Management)
- Case Development Workshop

Gain the knowledge and skills necessary to perform an in-depth analysis of your company's vulnerabilities for fraud in the areas of Interconnect and SIMbox.

## Overview

The domains considered in this class include some of the most confusing and complex situations ever created by man. In these areas, contracts, partner relationships, regulatory constraints and customer opinions and behaviors combine to make 'winning at partnering' a risk fraught endeavor under the best of conditions. In this class we will not only explain the intricacies of these relationships, their limitations and liabilities, but provide the student with a systematic discipline for understanding and addressing the Simbox and Interconnect.

By the end of this class, the student will be able to perform an in-depth analysis of their company's trafficking, partnering, regulatory and market vulnerabilities in the area of Interconnect and SIMBOX fraud, and will be equipped to develop meaningful solutions for the ongoing detection, deterrence and prosecution of these cases

**Duration:** 2 Days

## Who Should Attend?

Experienced Professionals and those who are new to Telcoms Fraud Management who are interested in learning about the fraud-sensitive areas of Interconnect, Bypass and SIMbox Fraud



## 2-Day Masterclass: Interconnect, Bypass and SIMbox Fraud

Day 1 (TFO102)	Day 2 (TFO103)
Network Foundations for Interconnect	Interconnect Operations
CDR Processing Principles (Mediation, Postpaid)	Regulators Dilemma - Interconnect Regulation
Fraud Management Systems Operation	External/Internal Interconnect Fraud
CDR - AAA (Authentication, Authorization, Accounting)	Denial of Revenue Attacks
Network Security/ Fraud Protection	Bypass Fraud/SIMbox Fraud

## Key Concepts include:

- ▶ Principles of circuit technology
- ▶ Key network controls and methods
  - Topology, Security, Control Protocol, Transaction Control, CDR Generation Sequence, CDR Generation, CDR Transport
- ▶ Media characteristics and controls (*wireless and wireline*)
- ▶ History of Circuit Technology
- ▶ Understanding SS7
- ▶ Mediation Operations
  - ▶ Mediation Fraud Management
- ▶ Postpaid Billing Operations
  - ▶ Postpaid Billing Fraud Management
- ▶ AAA (Authentication, Authorization, Accounting) for Network
- ▶ Network Fraud Controls and Methods
- ▶ Fundamentals of Interconnect Operations
- ▶ Interconnect Network Design and Constraints
  - ▶ Interconnect CDR Topologies and Billing Controls
- ▶ CDR security for interconnect
  - ▶ Trunk Group Security and controls
  - ▶ Interconnect routing table security, issues and controls
  - ▶ Settlement process operations, fraud risks and controls
  - ▶ Internal Interconnect Frauds and their Prevention
  - ▶ External Interconnect Frauds and Their Prevention
  - ▶ Denial of Revenue Attacks
  - ▶ Fundamentals of BYPASS Fraud and SIMbox Operations
  - ▶ Bypass Mapping and Assessment Approach

## GRAPA Fraud Officer Certification Credit

Successful completion of this course, testing and experience verification will result in the student being awarded GRAPA Fraud Officer Competency Credit for the following areas from the GRAPA Fraud Officer "Body of Knowledge":

- Principles of Network Operations and Management
- Wireless and Wireline Media Characteristics
- Billing Architectures and Controls
- Control Protocols Principles and Applications
- SS7 Principles
- Fraud Management System Fundamentals
- Advanced Fraud Management Systems
- Network Security and Fraud Protection
- CORE AAA
- Principles of Mediation Operations
- Principles of Post Paid Billing Operations
- Postpaid and Mediation Fraud Exploits and Remedies
- Principles of Interconnect Operations (Functions, Forensics and Controls)
- LOB Principles Interconnect
- External and Internal Interconnect Frauds
- Denial of Revenue Attacks
- Principles of SIMBOX operation, detection and deterrence
- Principles of BYPASS operation, detection and deterrence

Learn the Fraud-specific difficulties for Prepaid Roaming, as well as the basic functions of Convergent Billing Systems, CAMEL and more.

## Overview

Students in this course will learn the specific difficulties pertaining to the management, prevention and detection of fraud in Prepaid Roaming.

Learn the key operational characteristics of Roaming and Convergent Billing Systems, as well as the operational controls and fraud issues involved with Roaming.

Gain insight on the fraud management issues in Prepaid Roaming, CAMEL and more.

**Duration:** 2 Days

## Who Should Attend?

Experienced Telcoms Fraud Professionals as well as those who are new to the business who are interested in learning about the difficulties for Prepaid Roaming and Convergent Billing Systems as well as other fraud issues involved in Roaming Systems.



## 2-Day Masterclass: Roaming Fraud

Day 1 (TFO102)*	Day 2 (TFO105)
Network Foundations for Fraud Management	Postpaid Roaming Operations and Fraud Controls
CDR Processing Principles (Mediation, Postpaid)	USSD Roaming Operations and Fraud Controls
Fraud Management Systems Operation	Prepaid Roaming - Operations and Fraud Controls
CDR - AAA (Authentication, Authorization, Accounting)	Convergent Billing - Operations and Fraud Controls
Network Security/ Fraud Protection	Credit Frauds

## Key Concepts include:

- ▶ Postpaid Roaming Methods and Procedures
- ▶ HUR and NRTDE Roaming Credit Management
- ▶ Roaming SS7 Topology and Architecture
- ▶ Protecting against roaming traffic frauds
- ▶ Roaming clone frauds
- ▶ DCH role and frauds
- ▶ USSD Roaming Methods, operations and procedures
- ▶ Securing USSD revenues
- ▶ CAMEL Roaming - Operations, Controls and Fraud Risks
- ▶ Convergent Billing Systems Architecture
- ▶ Five categories of Convergence:
  - ▶ Billing Singularity
  - ▶ LOB Fusion
  - ▶ Rating Amalgamation
  - ▶ Credit Confluence
  - ▶ Account management unification
- ▶ Key fraud risks and containments in Convergent Billing
- ▶ Fundamentals of Interconnect Operations
- ▶ Interconnect Network Design and Constraints
- ▶ Interconnect CDR Topologies and Billing Controls
- ▶ CDR security for interconnect
- ▶ Interconnect routing table security, issues and controls
- ▶ Internal Interconnect Frauds and their Prevention
- ▶ External Interconnect Frauds and Their Prevention

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's "Body of Knowledge"

- Principles of Postpaid Roaming Operations (Functions, Forensics and Controls)
- Principles of USSD Prepaid Roaming (Functions, Forensics and Controls)
- Principles of Prepaid (CAMEL) Roaming (Functions, Forensics and Controls)
- Roaming Fraud Exploits, Cases and Remedies
- Roaming Fraud Management
- Convergent Billing Operations (Functions, Forensics and Controls)
- Convergent Billing Fraud Exploits, Cases and Remedies
- Principles of Network Operations and Management
- Wireless and Wireline Media Characteristics
- Billing Architectures and Controls
- Control Protocols Principles and Applications
- SS7 Principles
- Fraud Management System Fundamentals
- Advanced Fraud Management Systems
- Network Security and Fraud Protection
- CORE AAA
- Principles of Mediation Operations
- Principles of Post Paid Billing Operations
- Postpaid and Mediation Fraud Exploits and Remedies

Learn the how to handle frauds in these new lines of business, as well as how these new systems work and how they can be “fraud-proofed.”

## Overview

Become the Expert at your Telco for protecting New Technology Risks and Frauds

- Get up to date on the latest IP risks and ensure that you are protected from new waves of Internet fraud
- Learn the various methods for billing and operating 3G and GPRS and the risks and frauds associated with each
- Assure and fraud-proof your wireless network with confidence
- Discover why telecoms are becoming the favorite choice for money launderers, and how you can assure that your telco is protected against these criminals
- Stay ahead of M-banking technology and learn where the biggest risks can occur and the controls and techniques you need to safeguard your Telco

**Duration:** 2 Days

## Who Should Attend?

Anyone interested in Fraud risks associated with 3G, IP and GPRS as well as additional new lines of business, and how to detect and prevent frauds from occurring



## 2-Day Masterclass: 3G, IP and GPRS Fraud / Money Laundering

Day 1 (TFO204)	Day 2 (TFO205)
Network Frauds and Methods of Access	Packet Based Topologies and Architectures
Hacks, Phreaks and Attacks	SIP/VOIP and Packet Based Billing challenges
Core Telecoms Network	GPRS Operations, Billing and Frauds
Web-based Hacking	3G, Internet and IP Frauds
Attacks and Methods of Access (MOA)	Money Laundering for Telcos
LAN-Based Wireless Network	Mobile Banking Systems and Fraud Protection

## Key Concepts include:

- ▶ The Principle Domains, Exploits and Characteristics of Techno-Fraud
- ▶ Cyber-Terrorism and Phreaking
- ▶ Authentication, Authorization, Accounting
- ▶ Reference File Protection, Transaction File Protection
- ▶ Network Topology
- ▶ Major Techno-Exploits and Methods of Intrusion
- ▶ Credential and Identity Falsification
- ▶ Blackmail and Extortion
- ▶ Ethical Hacking
- ▶ Network Topology and Security
- ▶ ATM vs IP
- ▶ IP Protocol Family
- ▶ SS7 Review
- ▶ SIP and SS7 Relationship
- ▶ VOIP alternative business and billing models
- ▶ SGSN/GGSN Functions and Architectures
- ▶ APN Protection and APN Hacks
- ▶ PDP assignment and security
- ▶ Alternative GSN billing models
- ▶ Prepaid SGSN connections
- ▶ GRAPA standard GPRS controls and assurance
- ▶ Money Laundering and Banking Regulations
- ▶ Mbanking Architectures and Security

## GRAPA Certification Credit

Completion of this course of study, verified by testing, will earn attendees Competency Credit for the following areas in line with GRAPA's “Body of Knowledge”

- Network Intrusion Fraud Domain and Method of Address (MOA)
- Physical Network Security/Violation – Domains, Exploits, MOA
- Logical Network Security/Violation – Domains, Exploits, MOA
- Hacking – Techniques, MOA
- Phreaking – Techniques, MOA
- Customer Premise Equipment Violation – Domains, Exploits, MOA
- Logical Lease Domain Violation – Domains, Exploits, MOA
- Domain Review – Circuit Components: IN, MMSC, SMSC, WAP Server
- Domain Review – Packet Components: Email Server, Web Server, Content Server, Firewalls, Portals, Gateways, Radius Servers
- Domain Review – Radio Components: RNC, Node B, BTS, BSC
- MBanking
- Money Laundering
- NGN Security
- MGW Security
- GPRS Security
- SIP/VOIP Principles
- Packet Billing Models
- Principles of Packet Based Services and Billing
- SIP/Voip Operations and Principles
- VOIP Billing and Assurance
- Principles of GPRS Operations (Functions, Forensics and Controls)
- GPRS Security and Fraud Management
- Principles of 3G, LTE, UMTS and IMS (Functions, Forensics and Controls)
- 3g, LTE, IMTS and IMS Fraud management

# MORE THAN JUST TRAINING



# The Telco Fraud Academy EXPERIENCE!

## In the Classroom

## Out of the Classroom

**CHALLENGING CONTENT**



**SOCIALIZING**



**DISCUSSION**



**PARTICIPATION**



**CONFIDENCE BUILDING**



**NETWORKING**





Tel +1- 847-930- 3610  
Fax +1- 707-276-7676  
Email [info@grapatel.com](mailto:info@grapatel.com)



### 2010 Schedule:

Sep 2010	Kuala Lumpur, Malaysia
Oct 2010	Cape Town, S. Africa
Nov 2010	Dubai, UAE
Dec 2010	Chicago, USA

For the most up to date list of upcoming events,  
please visit our website:

[www.ra-academy.org/upcomingevents.htm](http://www.ra-academy.org/upcomingevents.htm)

We schedule courses and venues based on demand, so please be sure to tell us if you are interested in a particular class and location. We only move forward with our planning if there is enough interest. To make these trainings happen we need commitment from a minimum number of delegates. Please refer to our website for specific policies.

### About us:

The Telco Fraud Academy is the exclusive Telco Fraud training organization of GRAPA. GRAPA has over 4500 registered members and has distributed more than 3000 copies of its 2009 standards book. We have taught the Telco Fraud Officer and the Xtreme Revenue Assurance curriculum to over 600 GRAPA members. By offering events that combine benchmark development, sharing of standard practices and approaches, as well as delivery of workshops, the Telco Fraud Academy provides a unique and powerful venue for deployment of standard practices and rapid integration of those practices into the participating telco environments.

We have conducted our training programs for dozens of carriers and services providers around the world. Our workshops are offered in public venues (attended by delegates from many operators and services providers, which promotes the sharing of practices) as well as onsite for a private, more personalized and focused training for a company's staff.

### Some of what makes our training so unique:

1. Based entirely on the GRAPA standards of professional fraud deterrence and detection practices
2. Taught by Rob Mattison and Louis Khor, leading authorities on the practices of revenue assurance and fraud deterrence and detection in telecommunications.
3. Focused heavily on practical experience, not theory

Visit our website to read some great reviews from students who have attended our training:  
[www.ra-academy.org/Testimonial.htm](http://www.ra-academy.org/Testimonial.htm)

## The Instructors



**Rob Mattison**, world renowned expert in telecommunications and the revenue assurance industry, teaches all courses.

Rob has 20+ years of hands-on industry experience. He is President of the Global Revenue Assurance Professionals Association (GRAPA), author of *The Revenue Assurance Standards - 2009 Edition*, and of *The Telco Revenue Assurance Handbook*, which has become the authoritative guide for RA Managers at telecom firms around the world.



**Louis Khor**, has had a long career in education and management, with significant experience as a technology commentator and telecommunications analyst. Formerly a Senior Analyst with one of the premier telecoms research firms in the US, New Paradigm Resources Group (NPRG), Louis has authored reports on forward looking markets and technologies such as Fixed Wireless, Hybrid Fiber Coax(HFC)/DOCSIS 3.0 and Metro Ethernet. He has been responsible for research and curriculum development, and has been instrumental in setting strategic direction for the next phase of GRAPA's phenomenal growth.