

Certify as a

Telco Fraud Officer

CAIRO 2010

6-17 June 2010

Telco Fraud Officer Event Guide



**RA
Academy**

**Telco
Fraud Officer**



TFO001: Come and get it! Is your telco a Free Meal for Fraudsters?

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

TFO002: Techno Fraud, Cyber Crime and Phantom Phreaks : High Tech Fraud for the High Tech Telecom

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

TFO003: Broken Trusts: Customer and Employee Fraud

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

TFO004: The Prisoners Dilemma: Partner Fraud

Learn about interconnect, bypass, Simbox, roaming, Virtual Network Operator, Content partner and related partner frauds. Gain knowledge of how to understand and diagnose them, and how to deal with them

TFO005: Creating a Secure Environment: Dealing with Criminals, Terrorists and Law Enforcement

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



Get Certified This Week!

New GRAPA Pilot Certification Program



Register for this training and certification event at
www.ra-academy.org/revenue_assurance_training_events/Middle_East_1/revenueassurancetraining.asp



Courses Offered at this Event:

- TFO001 - Come and Get it! Is your Telco a Free Meal for Fraudsters?.....3
- TFO002 - Techno Fraud, Cyber Crime and Phantom Phreaks : High Tech Fraud for the High Tech Telecom.....4
- TFO003 - Broken Trusts: Customer and Employee Fraud5
- TFO004 - TFO004: The Prisoners Dilemma: Partner Fraud6
- TFO005 - Creating a Secure Environment: Dealing with Criminals, Terrorists and Law Enforcement7

The Revenue Assurance Academy Experience.....8

Contact Us / Event Schedule.....13



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 detect and deter 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 overall.

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. We will consider the 7 principle domains for fraud risk, provide a systematic diagnosis of each and review the top 100 exploits that are costing telecoms billions of dollars a year.

Duration: 1 Day

Who Should Attend?

- ▶ Experienced Telcom Fraud Management personnel
- ▶ People new to Telecoms Fraud Management
- ▶ Internal Auditors, CFO's, Security Specialists, Risk Officers and related Managers
- ▶ Regulators, Law Enforcement Officers, Government Security Officers and others interested in understanding the major issues, constraints, liabilities and capabilities of a typical telecommunications organization to partner and assist in law enforcement and other criminal/terrorist containment strategies



Key Concepts include:

- ▶ The Telco Fraud Officer Concept,
- ▶ Measuring Telco Fraud and Fraud Risk,
- ▶ Fraud Risk Assessment Methods,
- ▶ The Fraud Detection and Deterrence Lifecycle,
- ▶ Averse Accessory Fraud
- ▶ CRM and Sales Fraud
- ▶ Supply Chain and Inventory Management Fraud
- ▶ Partner and Bypass Fraud, Averse Accessory Fraud
- ▶ Administration and Accounting Fraud
- ▶ Operational Domain Knowledge,
- ▶ Target Decomposition Techniques
- ▶ Method of Ingress Analysis, Exploit Analysis
- ▶ Inventory of Exploits
- ▶ Case Studies in Fraud, Controls, Corrections, Prosecution, Investigative Techniques
- ▶ Development of Prosecutable Cases
- ▶ Fraudster Profiling
- ▶ Roles and Responsibilities of a Telco Fraud Officer
- ▶ Interface between TFO and Audit, SOX, Security, Revenue Assurance, Fraud Management, Law Enforcement, Regulators, Government Security and other departments
- ▶ The Revenue Assurance Lifecycle

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 internal (audit, revenue assurance, security) and external (law enforcement, regulatory, governmental) agencies and departments

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-increasingly fast pace. However, this race to market brings with it a significant amount of risk when it comes to fraud potentialities. While telcos are undeniably responsible for being the launching pad for these many different technological innovations, they are equally responsible for the fraudulent exposures that these innovations generate.

This one-day 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 different 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
- ▶ People new to Telecoms Fraud Management
- ▶ Internal Auditors, CFOs, Security Specialists, Risk Officers and related Managers
- ▶ Regulators, Law Enforcement Officers, Government Security Officers and others
- ▶ Anyone interested in understanding the full depth and breadth of fraud exposures that telcos and consumers are vulnerable to and the ways that these exposures are identified, protected and prosecuted



Key Concepts include:

- ▶ The Principle Domains, Exploits and Characteristics of Techno-Fraud
- ▶ Cyber-Terrorism and Phreaking
- ▶ I/T Security,
- ▶ COBIT, ISACA, SOX, IFRS, GAAP,
- ▶ Authentication, Authorization, Accounting
- ▶ Reference File Protection, Transaction File Protection
- ▶ Network Topology
- ▶ Principles of Circuit Technology
- ▶ Principles of Packet technology
- ▶ Major Techno-Exploits and Methods of Intrusion
- ▶ Hacking
- ▶ Credential Falsification
- ▶ Identity Falsification
- ▶ Several types of Hacking, 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

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)
- Revenue Stream Fraud Domain and MOA
- Security and Audit Standards and Organizations (ISACA, COBIT, SOX, IFRS, GAAP)
- I/T – Network Audit Methodologies
- Circuit Technology – Intrusion Portals (AAA, Transaction /Reference Data Violation)
- Packet Technology – Intrusion Portals (AAA, Transaction/Reference Data Violation)
- Physical Network Security/Violation – Domains, Exploits, MOA
- Logical Network Security/Violation – Domains, Exploits, MOA
- BSS (I/T Systems) 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 about the major categories of customer and employee 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 customers and employees.

There are many areas where the telco is especially vulnerable to fraudulent attack. The biggest areas 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 to do 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
- ▶ People new to Telecoms Fraud Management
- ▶ Internal Auditors, CFOs, Security Specialists, Risk Officers and related Managers
- ▶ Regulators, Law Enforcement Officers, Government Security Officers and others
- ▶ Anyone interested in understanding the full depth and breadth of fraud exposures that telcos and consumers are vulnerable to and the ways that these exposures are identified, protected and prosecuted

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, and Principle Exploits
- ▶ Case Management Discipline
- ▶ Case 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 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 about interconnect, bypass, Simbox, roaming, Virtual Network Operator, Content partner and related partner frauds. Gain knowledge of how to understand and diagnose them, and how to deal with them.

Overview

The “Prisoners’ Dilemma” describes a situation where you are forced to cooperate with a partner, but you never know when he is going to cheat you - but that’s okay, because he never knows when you are going to cheat him either. The “Prisoners’ Dilemma” is an exercise utilized by game theorists to describe the different situations where people will choose to either lie and cheat or tell the truth in order to help themselves get ahead. No scenario describes the condition of the telco in relationship to its partners better than this.

The domains considered in this class include some of the most confusing, convoluted, complex and difficult to decipher 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 will we 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 whole range of fraud scenarios represented.

Duration: 1 day

Who Should Attend?

- ▶ Experienced Telcoms Fraud Management personnel
- ▶ People new to Telecoms Fraud Management
- ▶ Internal Auditors, CFO's, Security Specialists, Risk Officers and related Managers
- ▶ Regulators, Law Enforcement Officers, Government Security Officers and others
- ▶ Anyone interested in understanding the intricacies and many overlapping regulatory, market, profit, fraud risk, criminal risk and partner risk scenarios associated with interconnect, bypass, simbox, roaming, VNO, content and other forms of major partnership



Key Concepts include:

Principles of revenue assurance for prepaid roaming, including USSD and CAMEL

- ▶ Domestic and International Interconnect
- ▶ Bypass Fraud
- ▶ Simbox Bypass
- ▶ VOIP Bypass
- ▶ Partner/Carrier Bypass
- ▶ Regulatory conditions to define bypass
- ▶ Legal and Illegal Bypass
- ▶ Building a case for the prosecution of bypass
- ▶ Reading Interconnect
- ▶ Roaming and Content Contracts
- ▶ Interconnect Bypass Case Development
- ▶ Exploits and Resolution
- ▶ DCH
- ▶ Content Contract
- ▶ Roaming Architecture
- ▶ Roaming Fraud Vulnerabilities
- ▶ Role of DCH in Roaming Fraud Management
- ▶ Roaming Fraud Exploits and Resolutions
- ▶ Content Fraud
- ▶ Intellectual Property Rights Liabilities
- ▶ Content Fraud Protection

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":

- Partner and Bypass Fraud Domain Analysis and Method of Address (MOA)
- Interconnect network topology, POI, POP, GMSC architecture and structure
- Interconnect routing, rating and SS7 security and activity
- Traffic analysis and Interconnect CDR Forensics
- Interconnect contract review
- Market and regulatory analysis of interconnect traffic patterns and techniques for fraud detection
- SIMBOX – presence, usage, detection techniques, case building and prosecution
- Bypass fraud, proof and prosecution
- Roaming Fraud Domain Analysis and MOA (Method of Address)
- Roaming Architecture and SS7 Control Protocols Sequence
- GSMA Roaming Agreement Hierarchy and Enrollment
- Roaming agreement review
- Content Fraud Domain Analysis and MOA
- VNO Fraud – Issues and Approaches
- Intellectual property rights management and liabilities

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

With the depth and breadth of exposure that a telecommunications company embraces, it is actually surprising that a large portion of the crime and terrorism is NOT MANIFEST within the environment. 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.

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
- ▶ People new to Telecoms Fraud Management
- ▶ Internal Auditors, CFOs, Security Specialists, Risk Officers and related Managers,
- ▶ Regulators, Law Enforcement Officers, Government Security Officers and others
- ▶ Anyone interested in understanding the telecommunication carriers' liabilities and capabilities in the areas of terrorism, crime and Averse Accessory Fraud.
- ▶ Anyone interested in understanding how to best organize, manage and administer the fraud officer function within the telco
- ▶ Anyone interested in understanding how to set up and administer a fraud management system



Key Concepts include:

- ▶ Averse Accessory Fraud Domains (Targets, Methods of Ingress, Exploits)
- ▶ Working with Law Enforcement Agencies
- ▶ Evidentiary Methods
- ▶ Prosecuting Fraud
- ▶ Bribery, Con Games
- ▶ Vmail Frauds
- ▶ Email Frauds
- ▶ Website Frauds
- ▶ Extortion
- ▶ Blackmail
- ▶ Building prosecutable cases
- ▶ Forensic Methods
- ▶ Setting up a Telco Fraud Officers Management Department
- ▶ Incident management and measurement
- ▶ Domain management and measurement
- ▶ Fraud Management Systems
- ▶ CALEA
- ▶ Fraud Management Systems Administration and Management

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 US 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
- Setting up the Telco Fraud Officer Function
- Bribery, Extortion, Con Games, Identity Theft and other forms of averse accessory fraud and telecom liabilities
- Fraud Management Systems – set up and utilization

MORE THAN JUST TRAINING



The Revenue Assurance Academy EXPERIENCE!

In the Classroom

Out of the Classroom





Tel +1- 847-930- 3610
Fax +1- 707-276-7676
Email info@grapatel.com



Tentative 2010 Schedule:

Mar 2010	Lagos, Nigeria
Apr 2010	Delhi, India
May 2010	Miami, USA
Jun 2010	Cairo, Egypt
Jul 2010	Kuala Lumpur
Sep 2010	Europe (TBA)
Oct 2010	Dubai, UAE
Nov 2010	North America
Sep 2010	Eastern Africa
Dec 2010	USA (TBA)

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

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 Revenue Assurance Academy (RAA) is the exclusive training organization of the Global Revenue Assurance Professional Association (GRAPA). GRAPA has over 3900 registered members and has distributed more than 2000 copies of its 2009 standards book. We have taught the Xtreme Revenue Assurance curriculum to over 500 GRAPA members. By offering events that combine benchmark development, sharing of standard practices and approaches, as well as delivery of workshops, the Revenue Assurance 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 revenue assurance practices
2. Taught by Rob Mattison, the world's leading authority on the practice of revenue assurance in telecommunications, winner of many awards for his work in this area, author of *The Revenue Assurance Standards--2009*, *The Revenue Assurance Handbook*, and dozens of whitepapers.
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

The Instructor



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.

