Telco Fraud Certification Training

TFA Telecom **Fraud** Academy

Five-Day Telecoms Fraud Training & Certification Event

GRAPA Learn more about GRAPA at www.grapatel.com

TABLE OF CONTENTS

Certification or Course Customization
Choose the Topics you Want Most or Attend the 5-Day Certification Program

The Unit-Based Curriculum Approach:

Based on student feedback, GRAPA has updated the Telecom Fraud training to meet a wider variety of student objectives. While the majority of our attendees look to GRAPA training to help them earn the industry-recognized Telecom Fraud Analyst Certification, more and more are now requesting a greater amount of flexibility and customization to their training experience.

To meet this need, we have re-structured our Venue Events with the new Unit-Based Approach. Each day of this event is now divided into two, stand-alone, four-hour units. Each unit is focused on a single topic, and contains its own training, workshop, and testing sequence. Students now have the flexibility to take all 10 units and this event and earn GRAPA Telecom Fraud Analyst Certification, or attend only those modules that best correlate to their learning objectives.

Results-Driven Training Approach

GRAPA programs are grounded in the day-to-day, real world activities of Fraud professionals. Those who attend our events return to work with measurably greater understanding, tools, and skills to face the challenges of their environment. In fact, in many ways we define the success of our training by the increased value alumni bring to their teams and organizations.

For this reason, as we communicate with prospective students, we will often request that they get sign-off from their manager on learning objectives and course results. By incorporating a manager's perspective, potential students will have the opportunity to confirm that the topics covered in training will make them immediately more valuable to their team and organization. Furthermore, it enables us to ensure that those issues most critical to our student's professional success are incorporated into the event. As you view the steps below for either the Certification or Customized Training program, you will notice that manager sign-off has become a critical step in this process.

I Want Fraud Analyst Certification:

Do you want to join the ranks of the 100+ GRAPA Certified Telecoms Fraud Professionals? You can earn this honor at this event by successfully completing all 10 of the Units listed below. Taken as a whole, this Certification Program will provide you with some of the most tested, practical, and logical ways to prevent fraud and deliver real value to your organizations.

Next Steps:
➢ Express interest in certifying at this event
➢ Complete the pre-training course objectives survey to clarify training needs
➢ Based on survey results, we will provide you with a comprehensive lesson plan for the event
➢ Verify your lesson plan with your manager to ensure that training objectives will be met
➢ Work with your faculty advisor and membership manager to complete your registration for this event

I Want to Customize My Training Program:

Do you have specific training objectives? Maybe you can only get away from the office for a limited time? With the unit-based approach, you can now take only those training sessions that are the most important to YOUR objectives! Best of all, GRAPA will recognize your unit-by-unit completion so that you earn recognition for those topics you have completed.

Next Steps:
➢ Express interest in attending this event
➢ Complete the pre-training objectives survey to help determine which units are best for you
➢ Based on survey results, we will help you build a customized lesson plan for the event
➢ Verify your lesson plan with your manager to ensure that training objectives will be met
➢ Work with your faculty advisor and membership manager to complete your registration for this event

Fraud Certification At-A-Glance

Session	Day 1	Day 2	Day 3	Day 4	Day 5
Morning Unit (4 hours)	Telecoms Fraud & Cyber Crime Standard Practices	Security Fundamentals for the Telecoms Voice Networks	Internet Cyber Crimes - Network Intrusion & Social Engineering	Interconnect Settlement & Injection Frauds	Roaming Fraud - IFRS, CAMEL & Credit Exploits
Afternoon Unit (4 hours)	Fraud Management Systems & Criminal Forensic Systems	Security Fundamentals for Internet Networks	Hacking Telecoms Systems - Network & Radio Side Intrusions	Interconnect Bypass, SIMBox & Diversion Frauds	Subscription Frauds, Customer Frauds & Credit Mgmt

GRAPA's 5-day Training Event for Fraud Professionals
Certification Program Information

Overview:
GRAPA's Telco Fraud Specialist Training is a 5-day certification and workshop event designed to provide attendees with a new, innovative, and comprehensive approach to the professional practice of combating fraud in telecoms organizations as defined by the proposed GRAPA fraud standards, governance model, methodologies and framework. GRAPA's approach is exploit-library-driven, grounding fraud professionals in real-world risks and exposures.

5-Day Program Objectives:
The 5-Day Certification Program will meet the following student learning objectives:

- Optimize your use of the FMS and add new categories of alarms for more comprehensive fraud protection
- Make the fraud protection and detection job more manageable
- Have more confidence that I am using the right techniques to defend my telco from major frauds
- Understand the biggest telecoms fraud risks, and build a strategy for end-to-end detection and deterrence

Certification:
Students who successfully complete a unit, will get credit for their work. Students must complete each of the ten specified units (40 hours), pass certification tests, and have at least 6 months of verified work experience in telecoms to be awarded certification as a Telco Fraud Analyst (TFA).

Who Should Attend:
The primary audience for this Certification Training consists of telecoms fraud professionals. This includes those working with the fraud management system, internal auditors, forensic/investigative/law enforcement/legal professionals, logical and physical security specialists, finance and business risk professionals as well as key operational managers in sensitive domains (billing, network, accounting, sales, supply chain, procurement, etc.).

Our Promise:
Students who take the training seriously, participate enthusiastically in activities, and pass the certification exams will be able to perform all practical applications listed under each course description.

Day 1- Telco Fraud Overview & IT Systems Security

Unit 1: Telecoms Fraud & Cyber Crime Standard Practices
Industry Standard Approach & Methodologies

Unit Overview:

This unit provides the student with a comprehensive overview of Telecommunications Fraud Management and Cyber Crime Prevention as unique disciplines. While most industries have a fraud management function and are vulnerable to cyber crime, the complex telecoms technologies, business models and operational environments require specialized Fraud Management and Cyber Crime professionals with unique skills and knowledge requirements. Discussion of GRAPA's standards-based framework and approaches to telecoms fraud management and cyber crime: the FISHbone methodology, Incident Management Lifecycle, Situational Profiling, Fraudster Profiling, Behavior Profiling, Juristictional analysis and others.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want a consistent approach to finding and preventing frauds

• I want to perform fraud forensics in line with industry standard methods

• I want to improve my fraudster profiling techniques

• I want to better explain to management what it means to be a fraud professional and get more appreciation for the job I am doing

• I want to develop the skill set I need to be more successful at detecting and preventing frauds

Unit 2: Frauds Management & Criminal Forensic Systems
Maximizing Fraud Management System Value and Efficiency

Unit Overview:

Learn the key functions and uses of fraud management and criminal forensic systems, what they are, how they are used, functionality, differences and comparisons between key vendors/software, how to buy a system, what to look for, how to benchmark different software/hardware configurations to fit your environment.

Application of advanced methods to the running of a fraud management system, including the use of advanced statistical analysis, neural networks, regression analysis, as well as key considerations in calibrating alarms, balancing false positives with detection objectives, demarcating responsibilities and KPIs for fraud analysts.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit:

• I want to optimize my current fraud management system and set more alarms to find more frauds

• I want to know what to look for/requirements for a new FMS

• I want to utilize a data warehouse to generate alarms that my FMS cannot do

Day 2 - Network Basics for the Fraud Manager: Circuit & IP

Unit 3: Security Fundamentals for the Telecoms Voice Networks
(Pssst....You Cannot Secure Your Telco Without This Information)

Unit Overview:
Get an overview of the OSS/Network environment specifically designed to meet the need of fraud and security professionals, as well as law enforcement, national security, judicial and regulatory personnel. Students will learn to deal with the technical environment from a business perspective, focusing on Authentication, Authorization and Accounting - specifically the production of transaction records and CDRs, as well as guarding against exposures in the physical and logical architectures.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want to stop theft of service on my voice network

• I want to stop fraudsters from taking advantage of my voice network

• I want to improve my techniques for finding the vulnerabilities in my network

• I want to understand how my organization's network can become a playground for fraudsters and how to improve security

Unit 4: Security Fundamentals for Internet Networks
IP Fundamentals for the Fraud Analyst

Unit Overview:
This unit provides the student with an overview of the fundamental principles of operation, security and protection of IP based and cloud services. This unit is prerequisite to anyone attempting to understand and secure Internet Services, GPRS, UMTS, LTE, IMS, Cable, Satellite, IPTV, VPN or any of the services based upon the IP architecture. This unit provides students with a comprehensive understanding of the practical implementation of AAA (authentication, authorization and accounting) controls for all IP environments.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit:

• I want to understand enough about the new Internet-based technology that I can secure the IP network from major frauds

• I want to know the new fraud exposures that come with migrating to an Internet business model

• I want to secure the Internet network environments

Day 3 - Hacking & Security for Radio and Network

Unit 5: Internet Cyber Crimes - Network Intrusion & Social Engineering
Protecting Customers, Society and The Telco

Unit Overview:
See how Fraudsters break into IP-based and cloud environments and how you can protect against it. Learn about phishing, zero day vulnerability attacks, VPN hacks, SQL Injection, Denial of Service Attacks, (windows, linux, website, e-mail, methods of incursion and fraud). See how fraudsters hack a PC, break a wifi encryption, and learn what you need to protect against it.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want to stop fraudsters and hackers from taking advantage of my IP network

• I want to feel confident in the security I have built into my organization's Internet environment

• I want to improve my forensics techniques for finding the vulnerabilities in my IP-network

Unit 6: Hacking Telecoms Systems - Network & Radio Side Intrusions
Traditional Telecom Hacks & Modern Wireless Fraud Protection

Unit Overview:
Learn how fraudsters perform theft of service, denial of service, and averse accessory fraud. See how they can manipulate internal reference data/databases and compromise junctions/gateways, tee-ins, and signal intercepts. Learn about breaking GSM encryption, SS7 traffic spoofing, SIM clones, handset attacks.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit:

• I want to prevent theft of service and adverse accessory fraud in my organizations

• I want to understand how fraudsters can take advantage of my radio network and what controls I can put in place to prevent this activity

• I want to understand the details of the most costly Radio-side frauds and become my organization's expert for methods of detection and deterrence

Day 4 - Partner Frauds, FMS & Data Mining

Unit 7: Interconnect Settlement & Injection Frauds
Securing the Interconnect Environment

Unit Overview:

In this unit we examine key operational, commercial and technical security concerns in the interconnect/long distance/international calling environment. We review how partners, internal fraudsters, and professional criminal gangs exploit the complexity of the technical and commercial environment to defraud the telco, potentially leading to large cash losses within very short windows of time. Even more frightening, thse often go undetected for months or years.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want to stop my organization from getting hit with a major Interconnect Fraud

• I want to make sure my interconnect environment has the controls in place to protect against major fraud exploits

• I want to be confident that my organization has strong fraud defenses against PBX and Trunk Group Frauds

Unit 8: Interconnect Bypass, SIMBox & Diversion Frauds
Fight Traffic Piracy

Unit Overview:

Detailed coverage of how interconnect traffic is diverted and hijacked in order to deprive operators of legal revenue. Special focus of SIMbox detection and prevention, as well as identifying key culprits and means of addressing bypass in a rationalized, cost-effective way. Discussion of other forms of traffic piracy, including spoofing of SS7 traffic, A-num scrubbing, etc. used to defraud operators.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit:

• I want to understand how my traffic is diverted from my network and how to secure my interconnect environment

• I want to know how to modify FMS alarms to more quickly and accurately find cases of Bypass Fraud

• I want a cost effective solution to addressing Bypass & SIMBox frauds

• I want understand how fraudsters hack my SS7 network and utlize controls to prevent these attacks

Day 5 - Roaming Frauds & Subscription Frauds

Unit 9: Roaming Frauds - IRSF, CAMEL Exploits
Securing the Roaming Environment

Unit Overview:

In this unit we tackle frauds in the roaming environment. Often extremely costly, these are some of the most complicated frauds in one of the most complex telecoms Lines of Business - especially those that have to do with the use of premium rate numbers or International Revenue Share Fraud (IRSF). Extensive focus on other roaming frauds involving partner mis-conduct and evolving frauds exploiting vulnerabilities in the prepaid CAMEL roaming architecture.

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want to make sure I am not missing large internal frauds that occur in my organization

• I want to understand how fraudsters commit IRSF and premium rate fraud so I can build a strategy to defend against these exploits

• I want to know how to leverage logical security standards to add an additional layer of security around my CAMEL roaming environment

Unit 10: Subcription Frauds, Customer Fraud & Credit Management
This Represents 80% of Most Fraud Analysts' Time and Attention!

Unit Overview:

Understand how fraudsters exploit customer identities, trick point of sale staff, generate false traffic, run premium rate exploits, perform call sells, and more. Learn the controls needed at the Point of Sale, in Network, at Billing, and over Marketing for new rate plans to prevent these fraudulent activities. Also, learn to utilize a fraud management system and fraud data warehouse to detect these frauds early. Learn the credit management lifecycle and the critical role of the FMS in containing credit risk and preventing bad debt (including leased line frauds).

Unit Learning Objectives Students who have the following specific training objectives should participate in this unit

• I want to set better alarms to catch and prevent customer credit frauds

• I want to improve my ability to detect premium rate exploits

• I want to understand what I can do to stop major corporate frauds before they occur

I want to know what patterns I should look for to catch point of sale frauds more quickly

Why We are the Leaders in Training Telco Professionals Around the Globe

Join the leading provider of fraud-focused certification training events. Featuring exclusive presentations, real-world examples of procedures, solutions, and strategies that have effectively reduced fraud issues for telcos around the world.

After three years of providing best-in-class certification and training workshops to hundreds of telecoms risk professionals around the globe, we are pleased to announce our improved course offering.

☑ **Depth of knowledge** – The topics and examples are "narrow and deep" rather than broad and vague, presenting you with focused, highly targeted information that adds real value.

☑ **Tailored content** – Training is adjusted to align the needs of the students to the available material. Students are asked to fill out "GRAPA Benchmark Surveys" to determine the level and nature of the training required. The survey results help us determine how well you know your own systems, and provide clues about what you need help with. The principles and practices taught are also applied to cable, satellite, wireless voice, SMS, MMS, IPTV, and MMDS with equal conviction, detail, and effectiveness.

☑ **Relevancy** – Class material is based on the foundations of GRAPA. GRAPA members from every geography, type of carrier, major type of technology, and carriers of all sizes review and approve these standard approaches. The material serves as the foundation for an industry standard approach that is applicable to everyone, and yet easily focused to the needs of specific sub-audiences.

☑ **Based on real-world situations** – The majority of the training is experience-based "standard practices" in revenue assurance, harvested from the many revenue assurance professionals who participate in "practices surveys," "strategy sessions," and other information-sharing events. Clear, specific deliverables are provided that apply to real-world situations. The material is never based on speculation, guesses, or unvalidated information.

☑ **Interactive** – The workshops are more than lecture sessions. RAA classes are participative and interactive and students are expected to proactively join in discussions, problem solve, and fill out benchmarks. Attendees have opportunity for much interaction with the instructor and other students. Lunch and breaks are devised to facilitate more intimate conversation.

☑ **Professional development** – Students master vocabulary needed for creating a sense of professional identity and opportunities with other like-minded people in the industry that share common goals and issues.

Louis Khor, known for his energetic, lively and enthusiastic presentations on Revenue Assurance and Fraud at industry events and conferences, brings that same motivational style to teaching what he loves most – helping telecoms revenue professionals understand how uniquely positioned they are to affect the ongoing success and profitability of their organizations.

Rob Mattison is a world-renowned expert in telecommunications and the revenue assurance industry He has 20+ years of hands-on industry experience. He is President of GRAPA and 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.

Pamela Noriega has been GRAPA's Regional Chairperson for Latin America since 2008. Her background includes extensive experience is Finance, Risk Analysis and Project Management in several industries, including Banking and Telecommunications. She is the lead faculty for the South American region, and provides GRAPA Training in both English and Spanish.

Detecting and deterring fraud with proven techniques and strategies

GRAPA

About GRAPA

The Telco Fraud Academy is the exclusive fraud training organization of GRAPA. GRAPA has over 7000 registered members and has distributed more than 3500 copies of its 2009 standards book. The Telco Fraud Specialist curriculum is the Telco Fraud Academy's latest offering, providing revolutionary and relevant material. 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 revenue assurance practices
2. Taught by Louis Khor, Director of Research at GRAPA and the chief architect of GRAPA's Telco Fraud Certification Program
3. Focused heavily on practical experience, not theory

Visit our website to read some great reviews from students who have attended our training:
http://telecom-fraud.org/telecom_fraud_academy_info/testimonials.html

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.

TFA Telecom Fraud Academy

For the most up-to-date list of upcoming events please visit our website:
www.telecom-fraud.org

2013 Tentative Schedule:

04-08 Feb. 2013	London, UK
11-15 Mar. 2013	Ghana, Africa
17-21 Mar. 2013	Dubai, UAE
15-19 Apr. 2013	Chicago, USA
06-10 May 2013	Cape Town, Africa

Telco executives rave about the courses....

"The course exceeded my expectations. I learned many methods to apply in the detection and control of fraud and revenue assurance. I am glad I participated in this course and I hope to apply every concept in my job. Thank you so much."

Fraud Analyst, Honduras

"Being recognized and certified by a well-respected group like GRAPA is really something very inspiring to continue my endeavor and passion in the field of protecting telcos in revenue leaks and frauds. GRAPA training and certification is a MUST to ALL Revenue Assurance and Fraud Management Professionals working in the Wireless as well in the Wireline Telco. This is, I think, the best organized body where professionals can acquire continuing learning in Revenue Assurance and Fraud Management."

Senior Specialist-Financial Audit, Philippines

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