TELECOM FRAUD ACADEMY

Interconnect Bypass & SIMbox Hammerhead

Fight Traffic Piracy

GRAPA

TABLE OF CONTENTS

Interconnect Bypass & SIMbox Hammerhead

Deprive Traffic Pirates of your Revenue Bounty

A new generation of telecommunications bypass fraud professionals have begun to appear in markets around the world. These specialists are technologically, operationally and geographically sophisticated in ways never before imagined by operating companies. The impact of these professional fraudsters is measured in the billions of US dollars and no carrier is immune.

The Interconnect Bypass Hammerhead has been established in order to create the impetus and opportunity for fraud-related professionals to:

a) Share experiences and best practices

b) Learn the latest trends and approaches for the systematic containment and measurement of bypass risk and loss

c) Create targeted initiatives to upgrade the protection of these revenues Participants will attain Hammerhead certification for participation in this event.

The workshop is delivered over a period of three days, and consists of a combination of best practices training, small working group strategy sessions, group presentations and solution development. The following pages provide sample agendas for each of these three days.

At the end of the event, each participant will be provided with worksheets and action plans, and will be expected to follow-up with the implementation of the work plans developed.

Interconnect Bypass Hammerhead - Sample Curriculum

Day 1	Day 2	Day 3
Bypass Mechanics	**Fraud Protection Techniques**	**Action Plans**
Bypass Variants & Mutations	Quantifying True Cost of Bypass	Strategic Scoreboard Action Plan
Revenue-Focused Bypass Prevention	Bypass, VoIP, SIP, Grey Routes	Margin-Focused Prevention
Bypass Lifecycle Case Studies	Arbitrage, Blending, IC Revenue	Balancing BI, FMS, Test Calls
Bypass Controls Scoreboard	Business Intelligence Controls	How Does the Fraud Mutate?
GRAPA Standard Control Methods	Fraud Management Systems	Internal Partnering Responsibilities
Interconnect Revenue & Margins	Test Call Detection Programs	Regulatory Lobbying

A Letter from the Instructor

Esteemed Interconnect and Fraud Professionals,

I wanted to take this opportunity to thank you for your interest in our Interconnect Bypass Hammerhead event.

The GRAPA faculty team and I are very excited about the opportunity to meet with you and your teams and assist in the development of focused, highly effective strategies for the containment of bypass fraud revenue losses in your market. Over the past few years, the severity and sophistication of bypass fraudsters has begun to reach epic proportion in many markets and this program has proved to be instrumental for many carriers in the development of unique and highly effective solutions.

What is most critical to your success, is the understanding that:

a. The risk of loss due to bypass fraud is both credible and significant across the entire line of business
b. That the effects while often significant can go undetected without serious detection investment on your part
c. That you have available to you all of the tools and skills required to put serious containment around the risk

What most carriers come to realize is that while they have everything they need to combat this fraud, their biggest problem is the lack of coordination and commitment on the part of all of the parties involved. The assignment of clear responsibility for all aspects of the fraud, and the conscientious follow-up on tracking and compliance is critical.Teaming within your organization, teaming with your partners, your regulator and your peer opcos all plays a role in the solution.

It is my objective, and the objective of our entire team to make sure that you come away from this 3 day workshop with:

a. A fresh and comprehensive understanding of bypass frauds, how they happen and how you can take specific and direction action to minimize your exposure
b. A good overview and understanding of how other organizations are addressing these same risks and those techniques that apply directly to your company
c. A set of action plans that will enable you to:
    a. Leverage the experience of your current bypass practices
    b. Develop teaming strategies between bypass and operational teams to mutually contain risks

It is also our hope and commitment that you come away from the event with new insights, a new attitude as well as a new set of relationships and resources that you can tap in your ongoing battle with these fraudsters.

Rob Mattison

ICB101: The Mechanics of Bypass Fraud

Bypass fraud is as old as the telecommunications industry itself and bypass fraudsters have spent years perfecting their craft. The new generation of VOIP services and products, enabled by desperate competitors, innovative alternative carriers, and exacerbated by unsophisticated regulators have driven a new generation of VOIP fraudsters to create a world where traditional voice carriers end up subsidizing the revenues for criminals while their own margins shrink.

In order to combat bypass fraud, you must first understand how it works.
We will invest this first day of the workshop in establishing and understanding of how the interconnect business works, and how fraudsters take advantage of these complex technical, business and regulatory relationships to make money. We will also establish some workshop time where smaller groups of people will come together to share their own experiences, knowledge and approaches, and share the information with the overall group.

Bypass Variants & Mutations	*Comprehensive coverage of the fraud methods and approaches used by criminals to defraud your telco of interconnect revenue, and how they mutate and adapt in response of deterence and detection activities*
Revenue-Focused Bypass Prevention	*An analysis of Bypass Prevention as a business problem that has one main objective: maintaining and maximizing interconnect revenue and margins*
Bypass Lifecycle Case Studies	*Real world case studies of successful bypass prevention teams, and the timelines and lifecycles they went through in wrestling with this problem in order to implement lasting and permanent end-to-end solutions*
Bypass Controls Scoreboard	*Creating a bypass prevention infrastructure within the organization that is ensures all aspects of the problem are being dealt with in a comprehensive way, and that the problem is being addressed and solved from all angles*
GRAPA Standard Control Methods	*The industry standard best practices for the combat of bypass, and their implementation throughout the telco environment, ensuring that quantification, sizing and return on investment numbers are truly accurate*
Interconnect Revenue and Margins	*A review of the Interconnect Business Model and revenue stream, and how bypass fraud can have a severe impact on those crucial revenues*

Key Points:

Assessing the risk of Bypass Fraud
Bypass Fraud Lifecycle and Controls
Industry Standard Controls for Bypass Frauds
Managing Interconnect Revenue Margins

Hammerhead Workshop Outputs:

Bypass experiences Control / Combat success methods

ICB102: Methods of Protection

While the number of different ways to perpetuate bypass fraud are great, there are actually a small number of very specific controls and methods required to manage most of them. The biggest problem with the combating of bypass fraud is the fact that when the fraudster is doing things right, you don't even know it is happening.

The GRAPA standard controls framework defines 4 layers of controls and tracking methods that will provide you with the best information available to assist you in the assessment and combating of bypass.

During this day, we will review each of the methods of control available, and then have break out sessions where that level of control and risk will be discussed.

The results will then be reported back to the entire workshop.

Quantifying True Cost of Bypass Frauds	*Industry standard methods for measuring, reporting and quanitifying bypass effects, losses, costs and return on investment*
Bypass, VoIP, SIP, Grey Routes	*Understanding the key tools, methods and approaches used by fraudster to perpetrate bypass, understanding their equipment, means and vulnerabilities*
Arbitrage, Blending, IC Revenue	*Revealing aspects of the Interconnect business model that are fundamental to understanding bypass, why it happens, how it can be stopped, and why the "nuclear option" is not always the best*
Business Intelligence Controls	*Using a Data Warehouse or Business Intelligence system as one of the primary tools for detection, deterrence and analytics around SIMbox and bypass prevention*
Fraud Management Systems	*Using a Fraud Management System to productionize and streamline detection, deterrence and analytics around SIMbox and bypass prevention*
Test Call Detection Programs	*Using test calls/test events/call attempts as a definitive means of detection, deterrence and analytics arounds SIMbox and bypass prevention, evaluating Test Call vendors, building a business case, proving return on investment, leveraging interconnect partnerships*

Key Points:

Industry standard methods for reporting bypass activit ies
Data Warehouse and BI for combatiing Bypass Frauds
How to get the most out of Fraud Management Systems
Building Test Call detection programs

Hammerhead Workshop Outputs:

BI Controls Strategy and Approach
FMS Assessment
Test Call Detection Strategy

ICB103 : Action Plans

Strategic Scoreboard Action Plan	*Refocusing the various prevention, deterrence and detection methods around meeting key objectives, ensuring completeness through use of a comprehensive strategic scoreboard*
Margin-Focused Prevention	*KPIs, management reporting, and return on investment quantification focused around margins and ensuring the integrity of revenue streams*
Balancing BI, FMS, and Test Calls	*Making use of and evaluating approaches around the various deterrence and detection methods, designing a coverage plan that is approapriate for your unique and specific telco environment*
How Does Fraud Mutate?	*Mapping strategies to plan when and how to take action with/against other carriers in your market, how traffic flows change as a result of deterrence and detection actions, who gains and loses when you increase preventative efforts*
Internal Partnering & Responsibilities	*Teaming with an internal "cross-functional working groups" to implement consensus-driven strategies against bypass*
Regulatory Lobbying	*Working with and educating regulatory bodies to ensure prosecution, working within outdated regulatory regimes, legal and commercial strategies in partnering with regulators*

On the final day of the workshop event, each of the teams will be asked to prepare action plans that address each of the levels of vulnerability, detection and containment covered previously.

Interconnect bypass fraud is a unique phenomena to each operating company and market. What may be a huge problem in one market may be trivial in another. It is key therefore, that each operating company conduct an exhaustive review of the risk that they face.

The day will be organized through a series of lecture/classroom sessions, followed by workshop sessions..

Teams will define plans for:

1. Appropriate and accurate assessment of bypass risk
2. Specific strategies and containment plans where applicable
3. Fraud Management System Assessment and Utilization
4. Assessment and Strengthening of SOX and Standard Controls
5. Assessment and Strengthening of risk assessment reporting
6. Market / Pricing Assessments
7. Margin Analytics
8. Interconnect Market Segmentation Analysis

Key Points:

Roles and Responsibilities Action Plan
Margin Analytics Plan
Revenue Analytics Plan
FMS Plan
Regulatory Action Plan

Hammerhead Workshop Outputs:

Workplans for each containment analysis area

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

☑ 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.

☑ 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.

The Hammerhead Experience

The GRAPA Hammer-Head program provides a process that makes it possible for people to quickly get up to speed on ALL ASPECTS of the Interconnect Bypass and SIMbox frauds, while at the same time allowing them to learn, integrate and apply the information in easy to manage steps. These steps include an orientation to Bypass Frauds, foundational training of standard practices and controls for managing these incidents, individual environment mapping and final verification.

The Hammerhead certification program is based upon the GRAPA standards for fraud and over four years of benchmarking and standard practices based information collected from telecoms around the world. This program provides credible and substantial support for professionals interested in safeguarding their telco's most valued assets - their revenue streams.

The Instructors

Rob Mattison, world renowned expert in telecommunications revenue assurance and fraud management. Rob has 20+ years of hands-on industry experience. He is the president of 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, 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.

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

About GRAPA

The Telecom Fraud Academy (TFA) is an exclusive training organization of GRAPA. GRAPA has over 6000 registered members and has distributed more than 3500 copies of its 2009 standards book. By offering events that combine benchmark development, sharing of standard practices and approaches, as well as delivery of workshops, the Telecoms 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.

GRAPA training is proven to help YOU put your Fraud Management Team at the leading edge of the new technologies, business models and revenue streams that are defining the future of telecommunications.

GRAPA

Tentative 2012 Training Schedule:

06-17 Feb	London, UK
27 Feb - 09 Mar	Singapore
12 - 23 Mar	Lagos, Nigeria
18 - 29 Mar	Dubai, UAE
07-11 May	Cape Town, South Africa
21-25 May	Chicago, USA
10-21 June	Dubai, UAE
22-26 Oct	Cape Town, South Africa
12-23 Nov	Dubai, UAE
03-07 Dec	Orlando, USA

For the most up-to-date list of upcoming events please visit:
www.telecom-fraud.org/telecom_fraud_academy_training/calendar/calendar.html

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