Course Outline

Comprehensive Training on Bypass/SIM Box Fraud Detection and Termination

Duration: 3 Days

Title: Comprehensive Training on Bypass/SIM Box Fraud: Detection and Termination

Duration: 3 day

Course Code: NSE-RA-704

Course Description:

This training course is designed to explain the mobile and fixed communications bypass fraud in-depth and present effective solutions for detection and termination of bypass fraud. This course examines key subjects including: Definition of fraud and its types along with defining interconnection operations in order to help attendees better understand how bypass fraud works. The course also examines additional key subjects including: SIM box Interconnect configuration scenarios, and most importantly presenting and examining the fraud detection tools utilized. This is a must-attend course for revenue assurance and fraud management professionals.

Course Objectives:

- Understand what is Fraud and its Types
- Understand the Interconnect Principles
- Define Bypass Fraud and Understand its Characteristics
- Comprehend SIM Box Interconnect Configuration Scenarios
- Learn the Bypass Fraud Detection and Elimination tools
- Comprehend the Deficiencies of Traditional Behavioral Detection tools
- Learn the Non-Passive Push Calls Methodology

Pre Requisite

Basic understanding of Fraud, Basic understanding of Networks and Interconnection

Who Should Attend?

Revenue Assurance and Fraud Managers/ Analysts /Consultants/ Implementation and Deployment Technicians/ Project Team Members/Researchers

Course Outline:

I. Telecommunications Fraud Overview

- A. Telecommunication Fraud Overview
  1. What is Fraud
  2. Motivation of Fraud
  3. Operators Risk Exposure
  4. New Access Methods
  5. Billing Systems and Processes
- B. Interconnection Overview
  1. Fundamentals of Interconnect Operations
  2. Interconnect Network Design and Constraints
  3. Interconnect Controls
  4. Forms of Interconnections
- C. Types of Fraud
  1. Illegal SIM Boxes
     - a. Motivation and Scale
     - b. Associated Risks
  2. Subscription Fraud
     - a. Motivation of Subscription Fraud
     - b. Associated Risks
  3. Roaming Fraud
     - a. Motivation and Scale
     - b. Associated Risks

4. Premium Service Fraud
    a. Projected Revenue Unearned
    b. Associated Risk
5. Internal Fraud
    a. Motivation of Internal Fraud
    b. Impact and Scale of Internal Fraud
6. Partnership Fraud
    a. Types of Partnership Fraud
    b. Interconnect Fraud Recognition
7. Pre-Paid Services Fraud Methods
    a. Risk Associated with Recharge Methods
    b. Methods to Curb Pre-paid Fraud

II. SIM Box and Bypass Fraud

A. What is Bypass Fraud
1. By Pass Fraud Direct Effect
    a. Huge Revenue Loss
    b. Poor Voice Quality
    c. Increase in Post Dial Delay
2. By Pass Fraud Indirect Effect
    a. Inability to Call Back
    b. Short Duration Calls
    c. Increase in Call Drops

B. GSM VOIP Gateways/SIM Boxes
1. What are SIM Boxes
2. SIM Box Functionality
3. Advanced SIM Box Features and Functionalities
    a. SIM-Rotation
    b. Remote Pre-Paid Recharging
    c. SIM-Card off-site Storage

C. Use of SIM Cloning for SIMBox/ByPass Fraud
D. Use of International Roaming for SIMBox/Bypass Fraud
E. Re-filing Numbers within SIMBox Fraud
F. Effect of Special Rates between International Interconnects
G. SIM Box Interconnect Configuration
   3. SIM Box Location: Adjacent Operator’s Network
      a. Adjacent Network Inbound Mobile Originated Calls Delivery
      b. Scenario Identification and Details
      c. Scenario Treatment Difficulty
      d. Soft Loss
      e. Cases and Examples
   4. SIM Box Location: In the Home Operator’s Network
      a. Adjacent Operator Outbound Mobile Originated Calls Delivery
      b. Scenario Identification and Details
      c. Outbound Termination Access Fees Payment
      d. Soft and Hard Loss Cases
      e. Cases and Examples
   5. SIM Box Location: Within the Home Operator’s Network
      a. SIM Box Delivers and Terminated Calls On-Net
      b. Network Concerns
      c. Quality of Service
      d. Congestion
      e. Spectrum Management
      f. Network Utilization
H. By-Pass Fraud Detection and Elimination
   1. Traditional Behavioral Detection Examples
      a. Incoming to Outgoing Calls Ratio and Comparison
         i. “Voice Call Accepting” GSM Gateway Configuration
         ii. “Duration of Call” Comparison Counter Measure

iii. “Pre-Recorded Messaged or Dial Tones”

b. No or Low Mobility

i. “Take SIMs for a Ride” Counter Measure

ii. Voice Call Making Location

c. Distinct Numbers - High Number of Calls

d. High Number of One Cell Subscribers

e. High Number of Night Calls

i. Placing GSM Gateways in Large Cells

ii. Disabling Not-in-Use SIM Cards

iii. Automatic SIM Mapping

2. Signaling-Based Monitoring

a. Behavior Dependent

b. Near-Real time Monitoring

c. Media Dependent

d. High Deployment Cost

3. Non-Passive By-Pass Fraud Detection and Elimination

a. Solution Methodology

b. Real-time Individual Calls Monitoring and Blocking

c. Media Independent

4. Trunk Data

a. Trunk Analysis

b. Method of Trunk Analysis

c. Advantage of Trunk Analysis

5. Detection and Elimination Tool Comparison

6. Case Studies and Exercises