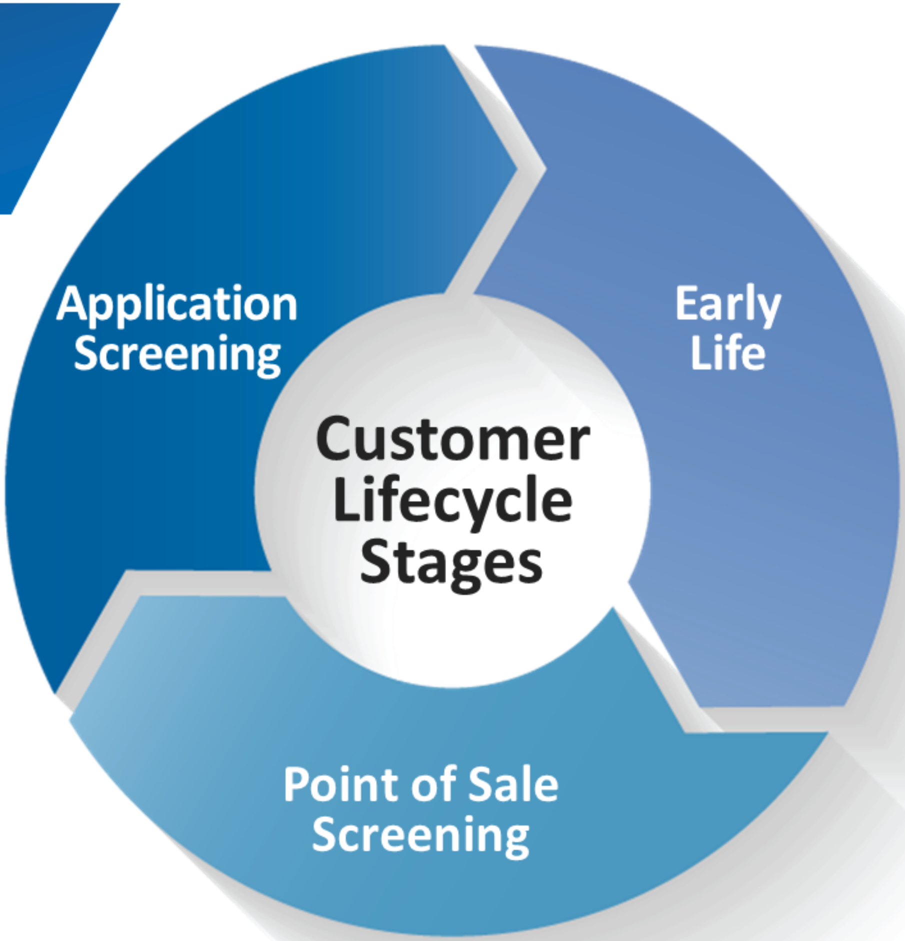
Solutions Across all Customer Lifecycle Stages

Acquisition (Offline)

- **Application Screening engine**
  - Matching negative DB Details
  - Fuzzy Logic on application details
  - Account change analysis



Early Life

- **Enhanced Fingerprinting Engine**
- **New Subscriber Evaluator (NSE)**
  - Immediate roaming
  - Null usage, initial calling pattern
  - Account change analysis

Acquisition (Real-Time)

- **Point of Sale Validation Solution**
  - Matching negative DB Details
  - Fuzzy Logic on application details

Point of Sale Validation Solution

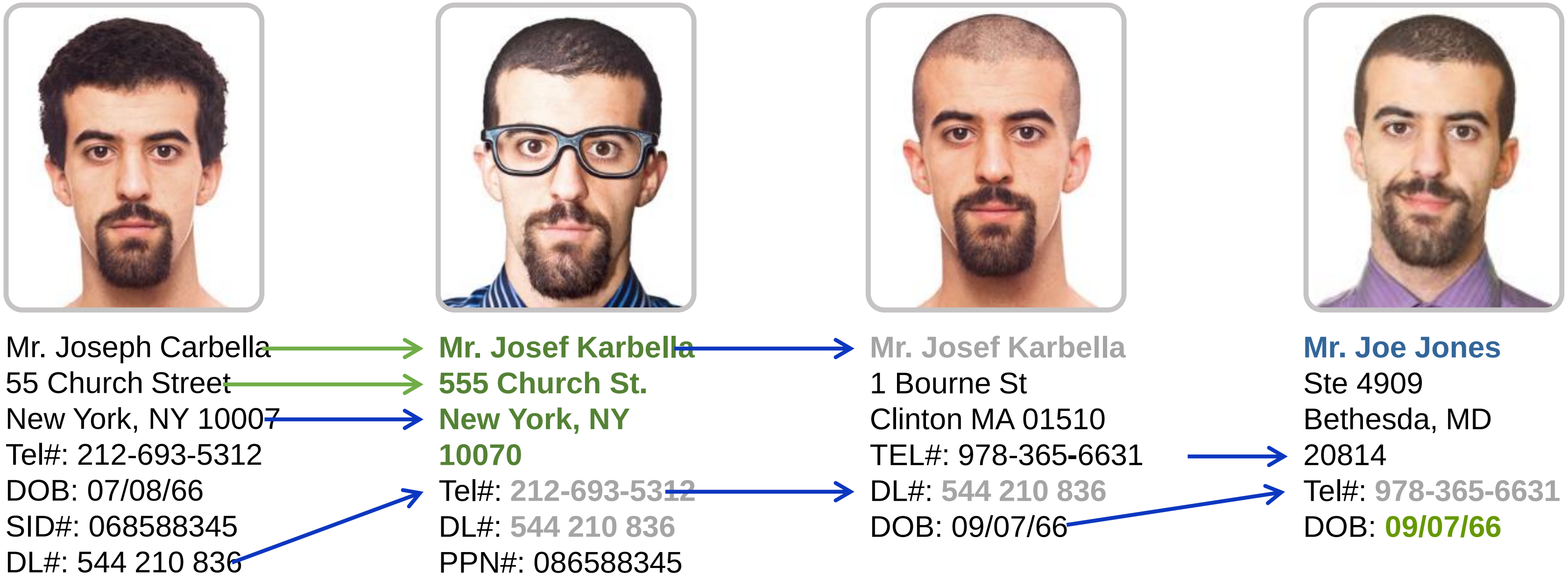
- **Verifies applicants at different point-of-sale channels** (sales outlets, web, IVR, etc.)
- **Provides immediate feedback** on whether to accept or deny the application, accept with restrictions, or involve back-office fraud investigation
- **Based on the following elements:**
  - Integration with the point-of-sale systems to receive service orders and provisioning events in real time and send analysis feedback back to the POS
  - Real-time analysis of fraudulent and risky applicants by employing customer details matching and service order pattern detection

Application Screening Engine

- **Monitors new applicants and applications** for new services to detect subscription fraud and returning fraudsters
- **Analysis performed is based on user configurable rules, on different levels:**
  - Analysis of a single service order (e.g., use of a bad credit card)
  - Analysis of service order patterns (e.g., purchase of multiple devices with different dealers in a short period of time)
  - Alias matching – Exact/Fuzzy matching of service order details to databases of known fraudsters, known bad debtors, etc.

Application Screening Example

Returning Fraudster – Alias Matching Example



Mr. Joseph Carbella
55 Church Street
New York, NY 10007
Tel#: 212-693-5312
DOB: 07/08/66
SID#: 068588345
DL#: 544 210 836

Mr. Josef Karbella
555 Church St.
New York, NY
10070
Tel#: 212-693-5312
DL#: 544 210 836
PPN#: 086588345

Mr. Josef Karbella
1 Bourne St
Clinton MA 01510
TEL#: 978-365-6631
DL#: 544 210 836
DOB: 09/07/66

Mr. Joe Jones
Ste 4909
Bethesda, MD
20814
Tel#: 978-365-6631
DOB: 09/07/66

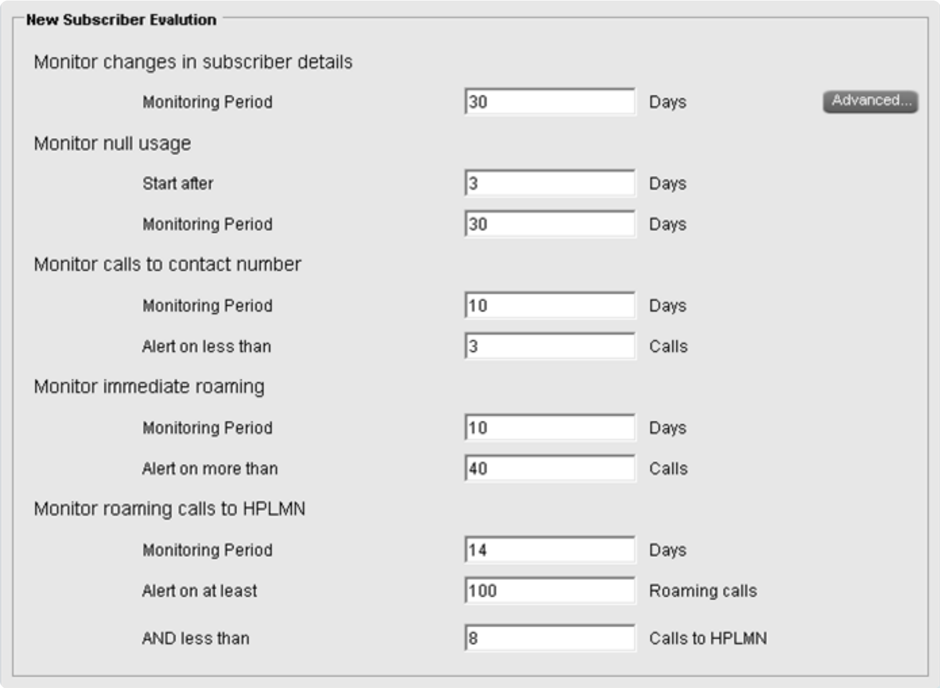
→ Fuzzy match
→ Exact match

Enhanced Fingerprinting Engine

- Stores usage “fingerprints” of all known fraudsters
- A “fingerprint” is a set of the most typical contacts used by the fraudsters (e.g., frequently called phone numbers)
- Monitors usage of new subscribers and detects returning fraudsters by matching their usage habits to fingerprints stored in the system’s DB

New Subscriber Evaluation Engine

- Detects possible fraud patterns at early stages of the customer lifecycle
- Detects patterns consistent with abnormal patterns that usually indicate the possibility of subscription fraud
- The analysis focuses on the following areas:
  - Suspicious subscriber details changes in proximity to activation
  - Null usage (‘silent subscribers’)
  - No calls to contact phone number
  - Suspicious immediate roaming usage
  - No calls to home carrier while roaming



New Subscriber Evalution

Monitor changes in subscriber details

Monitoring Period	30	Days	Advanced...

Monitor null usage

Start after	3	Days
Monitoring Period	30	Days

Monitor calls to contact number

Monitoring Period	10	Days
Alert on less than	3	Calls

Monitor immediate roaming

Monitoring Period	10	Days
Alert on more than	40	Calls

Monitor roaming calls to HPLMN

Monitoring Period	14	Days
Alert on at least	100	Roaming calls
AND less than	8	Calls to HPLMN

- Enterprise Fraud

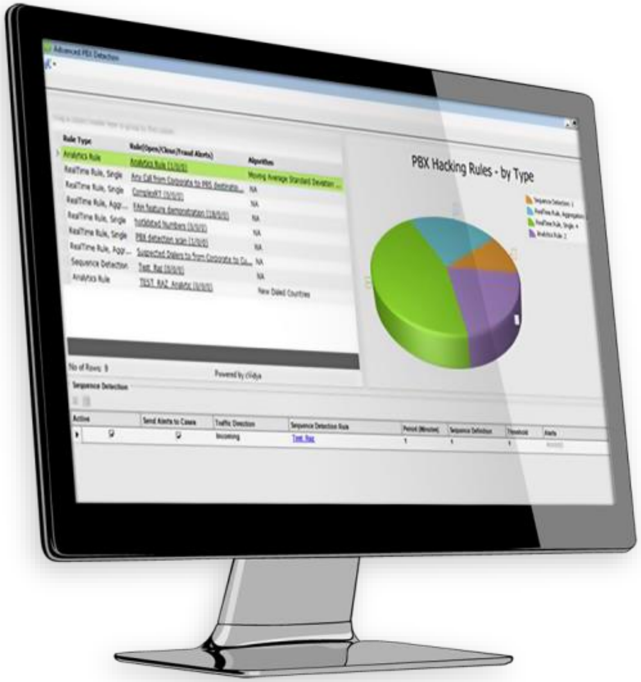
PBX Hacking

- **What is it?**
  - Fraudsters illegally hacking into a corporate automated phone system enabling them to dial into the PBX and generate outgoing traffic from the PBX to any telephone number (expensive destinations located overseas) at corporate expense
- **How is it done?**
  - Hackers gain access to the PBX in the following order:
    - Phone mail / voice mail
    - Remote Access or Direct Inward Service Access (DISA)
    - Remote maintenance/ Administration port
- **Relevant for operator types (located anywhere in the world) that offer fixed voice services to corporate customers that use PBXs**

Dedicated Solution for PBX Hacking

- **The challenge**
  - #2 fraud (CFCA – 2013)
  - Causing the industry annual damages of $4.42 B
  - The competitive telecom market forces operators to bear part of the losses when coming into a dispute
- **Amdocs's unique solution to PBX fraud – a combination of technology and expertise**
  - Dedicated detection schemes – predefined detection rules
  - A set of detection engines that identifies:
    - Sequential calling patterns
    - PBX profiling and changes in usage habits
    - Suspicious activities from within the PBX
  - Back-office investigation tools

Detection Schemes – Examples



Rule Type	Rule(Open/Close/Fraud Alerts)	Algorithm
Analytics Rule	Analytics Rule (1/0/0)	Moving Average Standard Deviation ...
RealTime Rule, Single	Any Call from Corporate to PRS destinatio...	NA
RealTime Rule, Single	ComplexRT (0/0/0)	NA
RealTime Rule, Agg...	FAH feature demonstration (18/0/0)	NA
RealTime Rule, Single	hotlisted numbers (0/0/0)	NA
RealTime Rule, Single	PBX detection scan (1/0/0)	NA
RealTime Rule, Agg...	Suspected Dialers to from Corporate to Cu...	NA
Sequence Detection	Test_Raz (0/0/0)	NA
Analytics Rule	TEST_RAZ_Analytic (0/0/0)	New Dialed Countries

No of Rows: 9

Powered by cVidya

Sequence Detection

Active	Send Alerts to Cases	Traffic Direction	Sequence Detection Rule	Period (Minutes)	Sequence Definition	Threshold	Alerts
☑	☑	Incoming	Test_Raz	1	1	1	[illegible]

- Calls from the PBX to known test numbers
- Suspicious activity from the PBX during non-activity periods
- Calls to risky countries/PRS destinations
- Changes in the PBX normal calling patterns
- Calls from the PBX to sequential number ranges

- Bypass Fraud Detection Solution

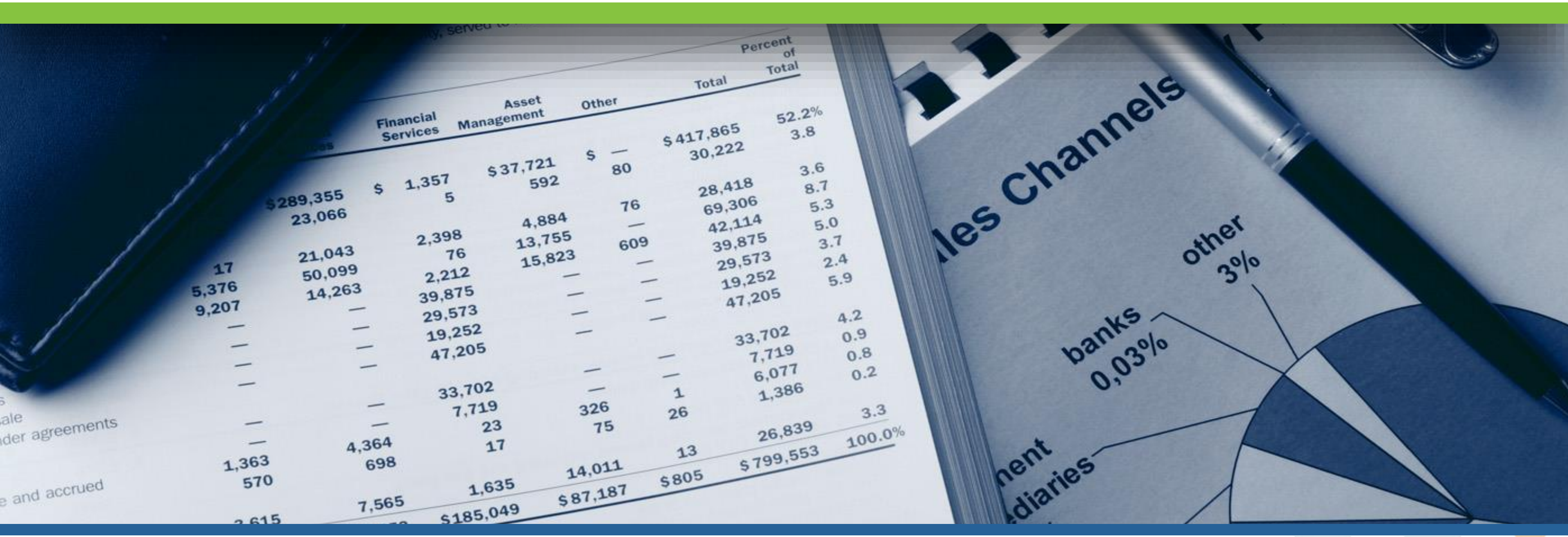
GSM Gateway/Bypass Fraud (SIMboxing)

- **What is it?**
  - GSM gateway is the establishment of a pseudo carrier type service without a license to operate and terminate international incoming calls as local calls
- **How does it occur?**
  - Setting up a VoIP infrastructure
  - Using a SIMbox with local SIM cards
  - Selling/offering cheap termination fees in the wholesale market
- **Relevant mainly in Central & Latin America, Caribbean, Asia Pacific, Africa and Eastern European countries**

Bypass Fraud Detection Solution

- **FraudView's solution for illegal bypass fraud:**
  - Automatic detection & prevention of bypass, including pro-active actions upon alert
    - Near-real-time – detecting fraud in less than an hour
    - Long term – detecting under-the-radar activities over weeks
- **Pattern analysis of Bypass-specific indicators, e.g.:**
  - Diversity of calls (Number of different calls/total number of calls)
  - Off-Net vs. On-Net Calls
  - Incoming vs. Outgoing Calls
  - Level of mobility (changes in cells)
- **Collaboration with test call generators**

• Sales Channels Fraud Detection



Sales Channel Fraud

AMDOCS REVENUE GUARD Powered by cVidya

- What is it?
  - An activity, which identifies loopholes in carrier’s incentives payments policy, and abuses these loopholes in order to be paid more
  - Any sale activity of equipment/service to the public, which bypasses carrier’s contract and which deprives carriers of revenues

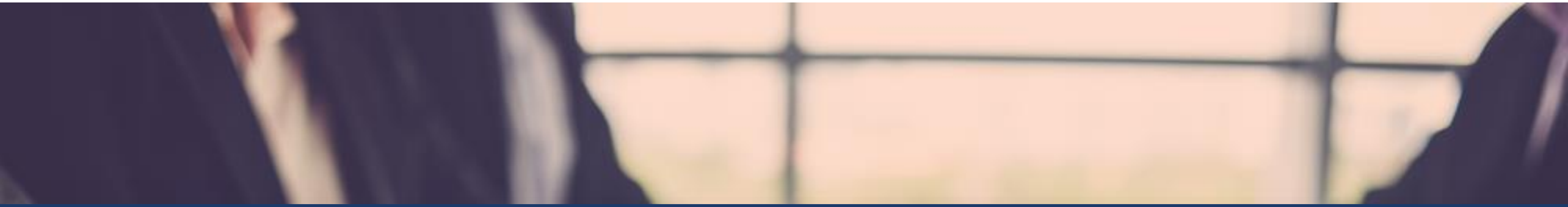
- How does it occur?
  - Poor visibility of carriers of their dealers’ sales behavior
  - Lack of monitoring techniques
  - Lack of investigation and analysis techniques
  - Lack of tools for automatic identification

- Very common in mature markets, where the increase in number of new subscribers is very moderate and dealers seek creative ways to increase their incomes

- May happen everywhere and affect any type of operator

Sales Channels Fraud Examples

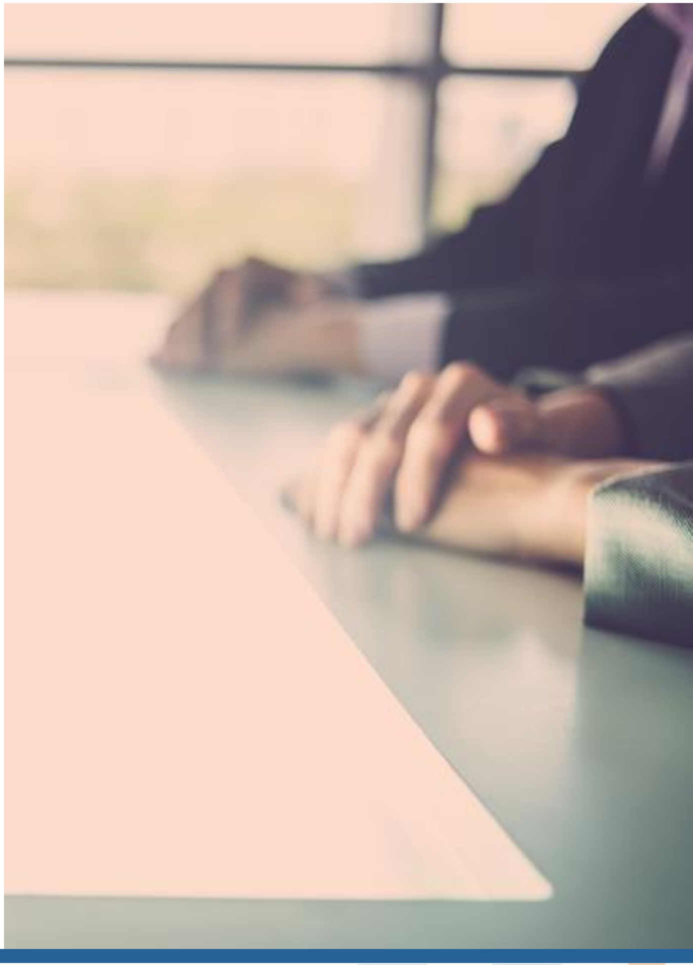
Fraud	Characteristics
Commission Manipulation	Dealers may overstate activity, falsifying entries or manipulating bonus periods or volumes to get higher commissions
Pack splitting/Commission Hopping	Equipment distributed to a dealer for retail as a single pack with a set bonus are split into their separate components and sold separately for greater commissions
Account Manipulation	Dealers sometimes change current account details to make it look like something has been sold. Changes can include unauthorized upgrades, addition of lines and additions of service
Account Splitting	Dealers will cancel an account and then re-activate that account to gain a higher bonus for a new account connection order rather than smaller bonuses for only a contract renewal order
Segment / Campaign Abuse	Sometimes packages targeted at specific populations / segments are offered and sold to ineligible customers in order to receive more commissions for the activations



- Back Office Fraud Detection

Back Office Fraud

- **What is it?**
  - Employees who exploit their familiarity with internal policies, procedures, technologies and their access to systems within the organization, to facilitate fraudulent attacks on the organization or its customers
- **How does it occur?**
  - Employee expertise in their area of responsibilities
  - Frustrated employees
  - Lack of clear internal policies
  - Lack of monitoring techniques
  - Lack of investigation and analysis techniques
  - Lack of tools for automatic identification
- **May happen everywhere and affect any type of organization**



Back Office Fraud Solution – Key Features:

- Combines FraudView's state-of-the-art detection and investigation capabilities along with accumulated business "Know-How"
- Provides various detection schemes including:
  - Rule based analysis (single and multiple records analysis)
  - Advanced statistical analysis capabilities:
    - Significant deviation from normal habits of an entity
    - Comparison of entity's behavior to its Peer group
    - Ratios
  - Same employee, same customer relations
  - Use of Hot lists
  - Multiple violations made by the same entity
  - Strange ID detection

- Why FraudView?