Fourth ITU Regional Workshop for Africa
"Strengthening ICT Integrity: Combating Counterfeits, Testing Challenges, and Fraudulent Communications in Africa Region"
Tunis, Tunisia, 1 October 2025

SESSION 3: COMBATING FRAUDULENT COMMUNICATIONS IN THE REGION

FRAUD MANGEMENT

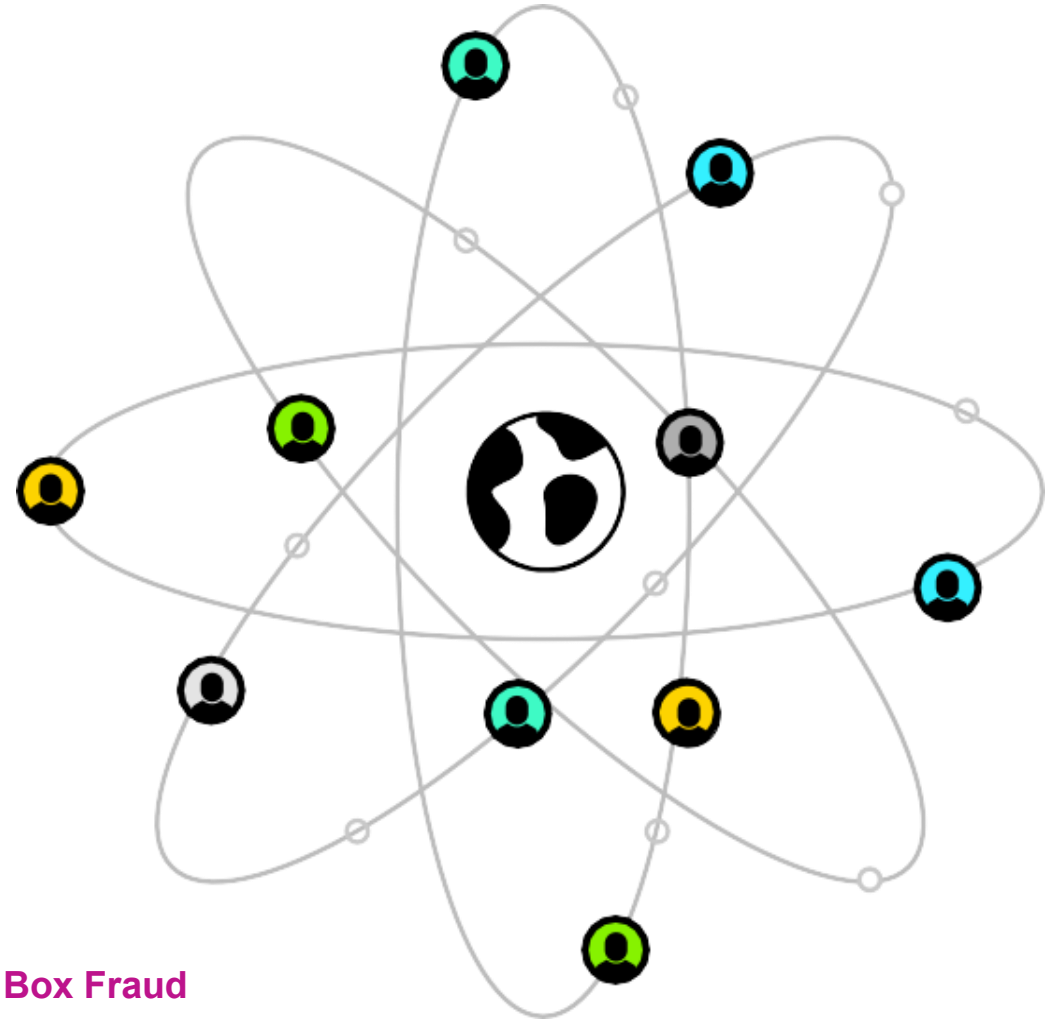
Presented by:

Mohamed MNIF
Senior Computer Engineer
RA & anti-Fraud Executive Director

FRAUD MANAGEMENT (DEFINITION & IMPACTS)

Subscription Fraud

International FRAUD



Roaming Fraud

PABX Fraud

SIM Box Fraud

FRAUD MANAGEMENT (DEFINITION & IMPACTS)

The intentional action of an individual, a group of individuals, or a company to receive products, services, and/or revenue from the target service provider without paying the expected value for those products or services.
The target may also have as potential impacts:

Commercial

- Disruption of business growth conditions
- Destruction of brand reputation

Technical

- Disruption of service
- Unsatisfactory quality of the service

Financial

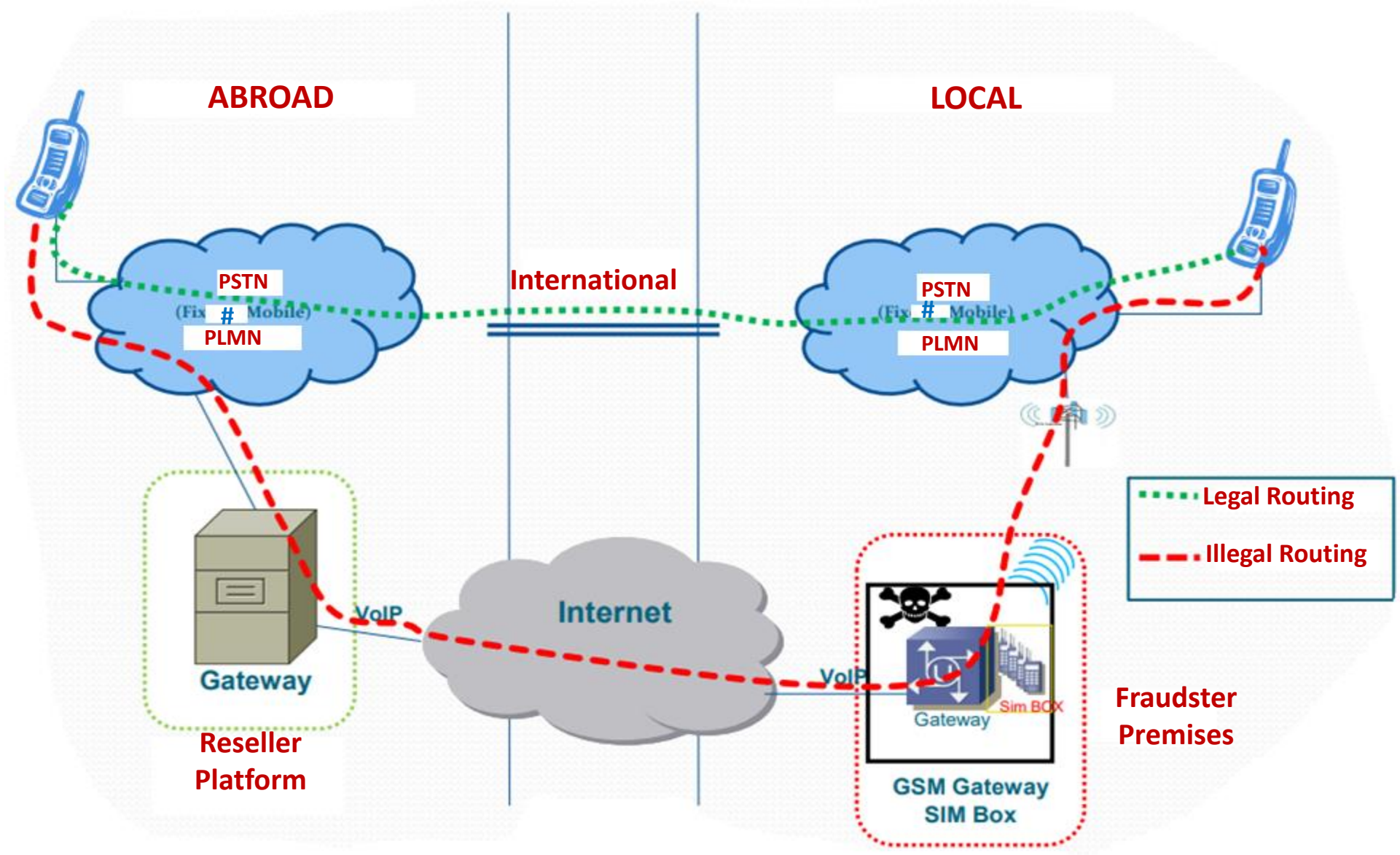
- Loss of revenue
- Increased costs
- Approximately **5%** of revenue is lost each year; roaming fraud accounts for approximately **24%** of total fraud

BYPASS Or SIM Boxing Fraud

- This is a call routed to bypass interconnection charges. A SIMBox is a device that diverts an international voice call via Internet Protocol (VoIP) to a SIM card of the mobile operator receiving the call. The international call appears to the terminating operator as a domestic call instead of an international call. Fraudsters make profits from this and operators lose international interconnection revenues;

- Technically, this is any incoming international call that ends up in a public telecommunications network as a domestically originated call without passing through dedicated international traffic circuits.

ARCHITECTURE OF A BYPASS VOICE CALL



BYPASS Or SIM Boxing Fraud

How to detect and limit SIM Boxing

1- Implementation of various systems based on different techniques (TCG) and profiling analysis of call tickets,

2- Reduction of latency in sending numbers for suspension, using techniques such as APIs and web services,

3- Reduction of fraudulent SIM detection time in order to decrease the MOU (Minutes of Use), with the integration of intelligent algorithms enabling **preventive** detection even before a call is made,

4- Close collaboration with other operators to facilitate and accelerate the suspension of off-net numbers,

5- Automated process implementation in order to applying sanctions, with collaboration between the Anti-Fraud Department, the Marketing Department, and IT Department. This process aims to ensure the accurate application of sanctions, enhancing policy compliance,

6- Periodic submission by the Anti-Fraud Department to the Marketing Department of sales reports confirmed to be fraudulent, splitted by regional department, distribution channel, and point of sale (POS), in order to deactivate suspicious POS codes and blacklist suspicious sellers,

7- Adopting a clear process to ensure clean distribution with the necessary accuracy, implementing applicable sanctions, defining thresholds for deactivating fraudulent POS, and limit the number of SIM cards owned by subscribers.

International FRAUD

International fraud involves fraudulent activities that occur across international borders. These frauds exploit vulnerabilities or weaknesses in global communication networks, often resulting in financial losses and security risks. Here are some common types:

1- International Revenue Share Fraud (IRSF): Fraudsters exploit the revenue-sharing mechanisms between telecom operators for international calls. They set up premium rate numbers and generate traffic through these numbers, earning a share of the revenue,

2- Roaming Fraud: Fraudulent activities exploiting international roaming services, such as using PsP SIM cards to make international calls without paying roaming charges or manipulating roaming agreements to gain unauthorized access,

3- Wangiri Fraud: This type of fraud involves missed call scams where international callers dial numbers and hang up after one ring. When the target calls back, they are connected to premium rate numbers, resulting in inflated call charges.

Detecting and preventing international telecom fraud involves sophisticated monitoring systems, collaboration between telecom operators, and the implementation of stringent security measures.

1 IRSF FRAUD

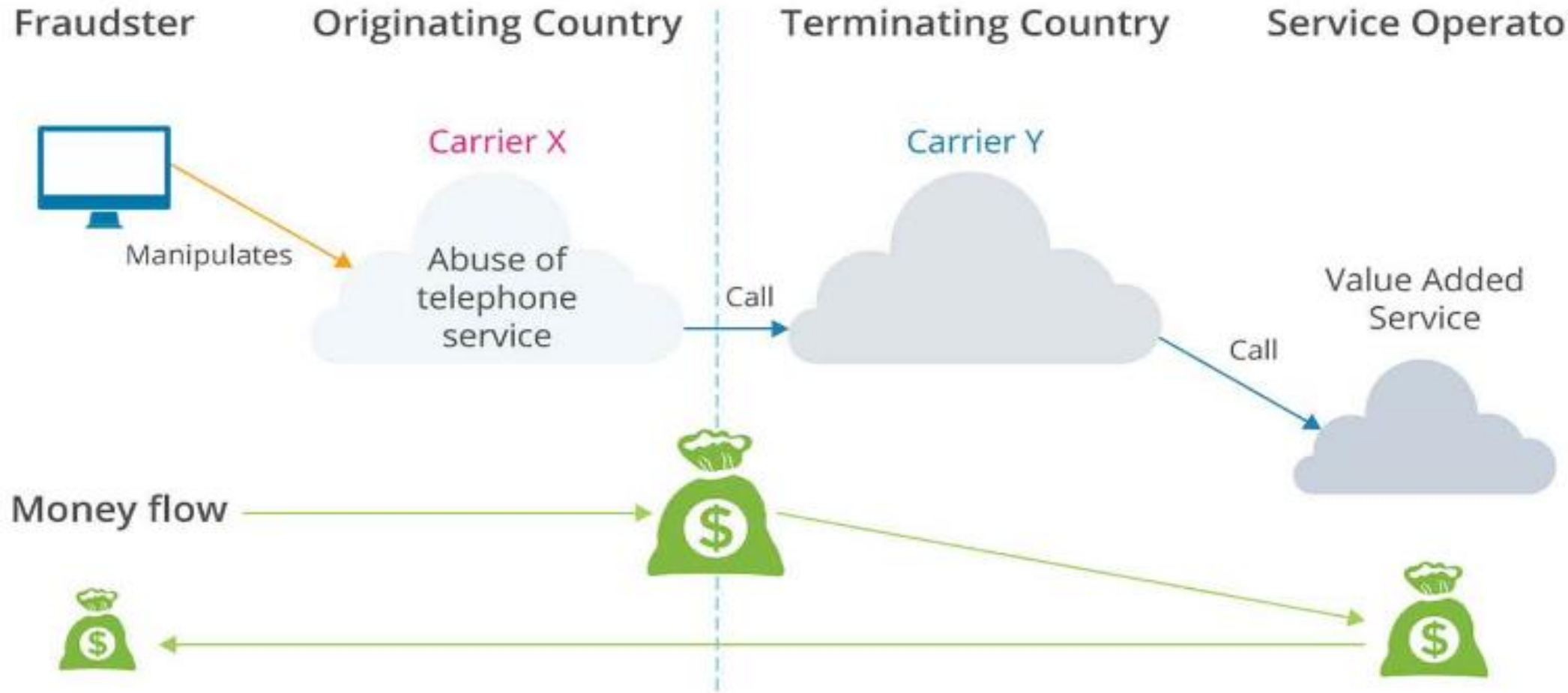
Fraudsters take advantage of the revenue generated by call termination rates to a few countries and collect a share of the revenue generated by incoming traffic for specific, usually international numbers.

Key aspects of IRSF:

1.Premium Rate Numbers (PRN): Fraudsters set up premium rate numbers that charge significantly higher rates than standard calls. These numbers can be located in various countries and often have prefixes that indicate high charges.

2.High Call Volumes: Perpetrators use different tactics to drive high volumes of calls to these premium rate numbers. They may employ auto-dialers, robocalls, or even hijack legitimate accounts to make numerous calls to these numbers.

3. Global Nature: IRSF is not confined to one country or region; it operates on an international scale. Fraudsters take advantage of the interconnected nature of telecommunications systems to perpetrate these scams across borders.


Fraudster
Originating Country
Terminating Country
Service Operator
Carrier X
Carrier Y
Manipulates
Abuse of telephone service
Call
Call
Value Added Service
Money flow

How to detect IRSF Fraud

1. Call Pattern Analysis: Telecom companies analyze call patterns to detect unusual call volumes, sudden spikes in traffic, or specific number patterns indicating potential IRSF activities,

2, Real-Time Monitoring: Utilizing real-time monitoring tools to track call traffic and patterns helps in identifying fraudulent activities as they occur, allowing for swift action to block or mitigate the impact,

1. Collaboration and Information Sharing: Telecom companies collaborate with each other and share information about known fraudulent numbers or patterns to prevent IRSF on a broader scale.

2. Roaming FRAUD

Roaming fraud involves exploiting roaming services, which enable users to access mobile services while traveling outside their home network's coverage area. This fraud concerns any subscriber registered for the roaming service who has made a certain number of calls and/or DATA connections over a period of 24 hours, exceeding the limit set by his home operator. Each operator sets the maximum amount that its roaming customers must not exceed.

Example: For Tunisie Telecom: 50 SDR
Reference: PRD AA 14 (Permanent Roaming Document of the GSM Association)

However, roaming fraud has its own characteristics, which include:

1. **Longer detection time** for fraud because it is committed on a network other than our operator,

2. **Also, longer response time** once the fraud is detected. The administrative and technical challenges of preventing it from continuing are greater.

3. **The technical challenges** of resolving fraud are more complex due to the diversity of the HPMN and VPMN networks involved.

To overcome these problems, we have implemented appropriate systems and processes, such as the FMS system and the consideration of flows from the NRTRDE, CDR's, as well as the HUR reports or bulletins communicated by the various operators.

3. Wangiri FRAUD

Wangiri fraud is a type of telecom scam that involves missed or one-ring calls. Fraudsters engage in Wangiri fraud by dialing a large number of random or sequential phone numbers, letting the phone ring just once, and then hanging up. The aim is to entice the recipient to call back the missed call.

Key characteristics of Wangiri fraud:

1.One-Ring Calls: Fraudsters use auto-dialing systems to make calls to a large number of random or sequential phone numbers, allowing the phone to ring just once before disconnecting.

1.Short-Duration Calls: The goal is to prompt the recipient to call back out of curiosity or concern,

2.Revenue Generation: The fraudsters profit from the high charges associated with international premium rate numbers, as they receive a share of the revenue generated from these calls.

To combat this type of fraud, we are deploying

1. Education and Awareness: Informing users about the risks associated with returning missed calls from unknown or international numbers can prevent them from falling victim to the scam,

1.Blocking Suspected Numbers: Blocking suspected Wangiri numbers, preventing them from reaching potential victims.

PABX FRAUD

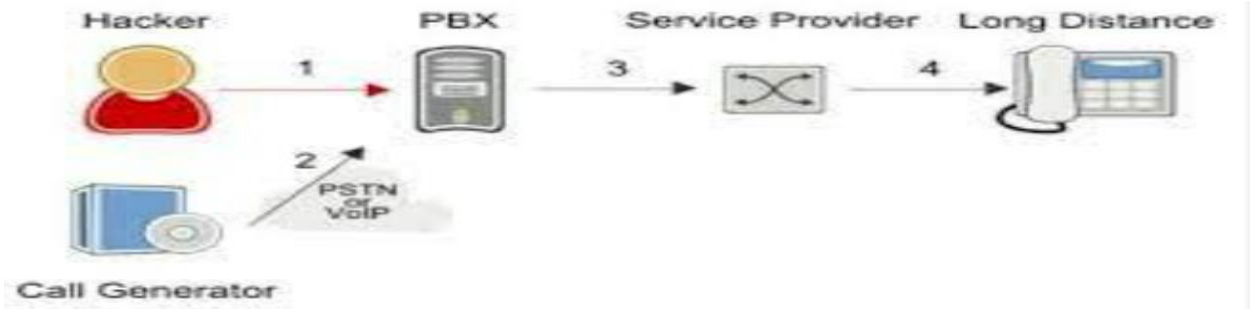
PBX hacking allows fraudsters to take control of phone lines by exploiting unsecured phone networks. A PBX (private branch exchange) is a private telephone network that connects to external networks. Since many of these PBXs are IP-based, they can be an easy target for hackers. This is a cybersecurity and IT problem that can be avoided with better internal controls and password security.

Key aspects of PABX fraud:

1.Hacking PABX Systems: Fraudsters gain unauthorized access to a company's PABX system, either by exploiting security vulnerabilities, using default passwords, or through social engineering tactics.

2.Call Routing Manipulation: Once access is gained, fraudsters manipulate call routing settings to make international or premium rate calls, often at the expense of the targeted company.

3.Call Forwarding and Redirecting: Fraudsters may set up call forwarding or redirect calls through the compromised PABX system to other numbers, including international or premium rate numbers, resulting in substantial charges for the affected organization.



PABX FRAUD

How to prevent PABX Fraud

1.PBX monitoring: based on the nature of the customer and their business, and the analysis focuses on call automation, the destinations called, and call times, which are generally, 99% of the time, outside of the company's administrative hours. Our goal is to detect these cases as quickly as possible, address them promptly, and thus alert our customers so they can further secure their access,

2.Strong Security Measures: Implementing robust security protocols, regularly updating passwords, and restricting access to the PABX system helps prevent unauthorized entry,

3.Regular Monitoring: Constantly monitoring call patterns and usage helps detect unusual spikes in international or premium rate calls, indicating potential fraudulent activity,

4.Call Restrictions: Implementing call restrictions, especially on international and premium rate numbers, can prevent excessive charges due to fraudulent activities.

Spamming FRAUD

Spamming fraud in the telecom industry involves the dissemination of unsolicited and often deceptive communications through various channels such as phone calls, text messages, and emails. These fraudulent activities aim to deceive recipients, often for financial gain or to extract personal information.

Key aspects of spamming fraud in telecom:

1.Phishing: Fraudsters use deceptive messages, pretending to be from legitimate sources like banks, government agencies, or reputable companies, to trick recipients into revealing sensitive information such as passwords, credit card numbers, or personal details.

2.Smishing/ Vishing : This form of fraud involves sending fraudulent text messages, often containing links or prompts for recipients to provide personal information or visit malicious websites.

3.Scam Calls: These are unsolicited calls where fraudsters use various tactics such as offering fake prizes, threatening legal action, or posing as tech support to scam individuals out of money or sensitive information.

Spamming FRAUD

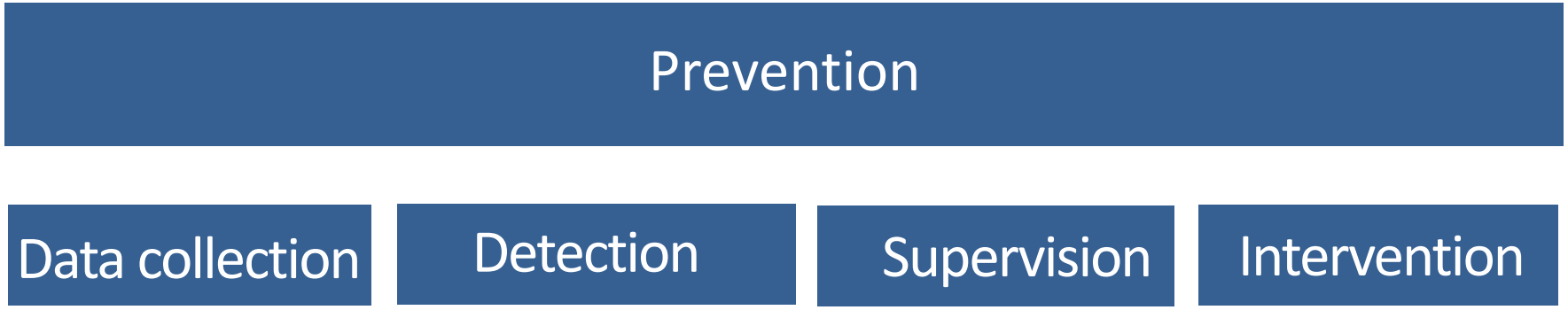
How to detect Spamming FRAUD

1.Call and Message Filtering: Implementing filtering mechanisms to identify and block suspicious calls and messages helps reduce the number of fraudulent communications reaching users.

2.Education and Awareness: Educating users about common fraud tactics, advising them not to respond to unsolicited messages or calls, and promoting awareness about how legitimate organizations communicate can help prevent falling victim to scams.

3.Blocking and Reporting: Allowing users to block numbers, report spam messages or calls, and providing mechanisms for reporting fraudulent activities to telecom authorities or service providers helps in curbing spamming fraud.

FRAUD PROTECTION PROCESSING & TOOLS



Fraud protection processes should minimize both the possibility of being a victim of fraud and the impact of fraud if ever it has occurred.

These processes are prevention, data collection, detection, supervision (monitoring) and intervention (response).


Thank You