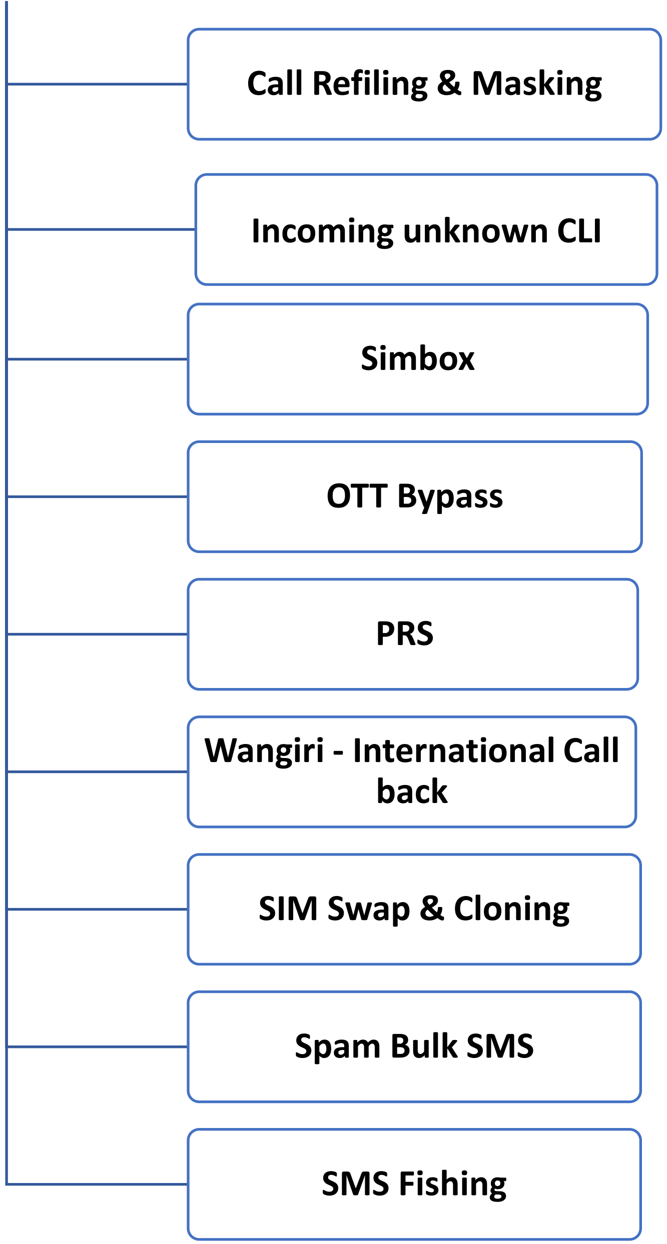
Deemed Impermissible Traffic

الجهاز القومي لتنظيم الإتصالات
NTRA
NATIONAL TELECOM REGULATORY AUTHORITY
NTRA
NTRA
NTRA
NTRA

Impacts of Deemed impermissible traffic

- Difficulties and Vulnerabilities in security, privacy and lawful interception requirements
- Economic losses occur due to non-collection of transit fees for incoming and outgoing international voice minutes through licensed international gateways
- Scamming the receiving parties of otherwise calls due to non-display of actual calling numbers (CLI)
- Violation of consumer rights by enforced usual deterioration of QoS/QoE against the will or without knowledge of the caller and/or the callee.

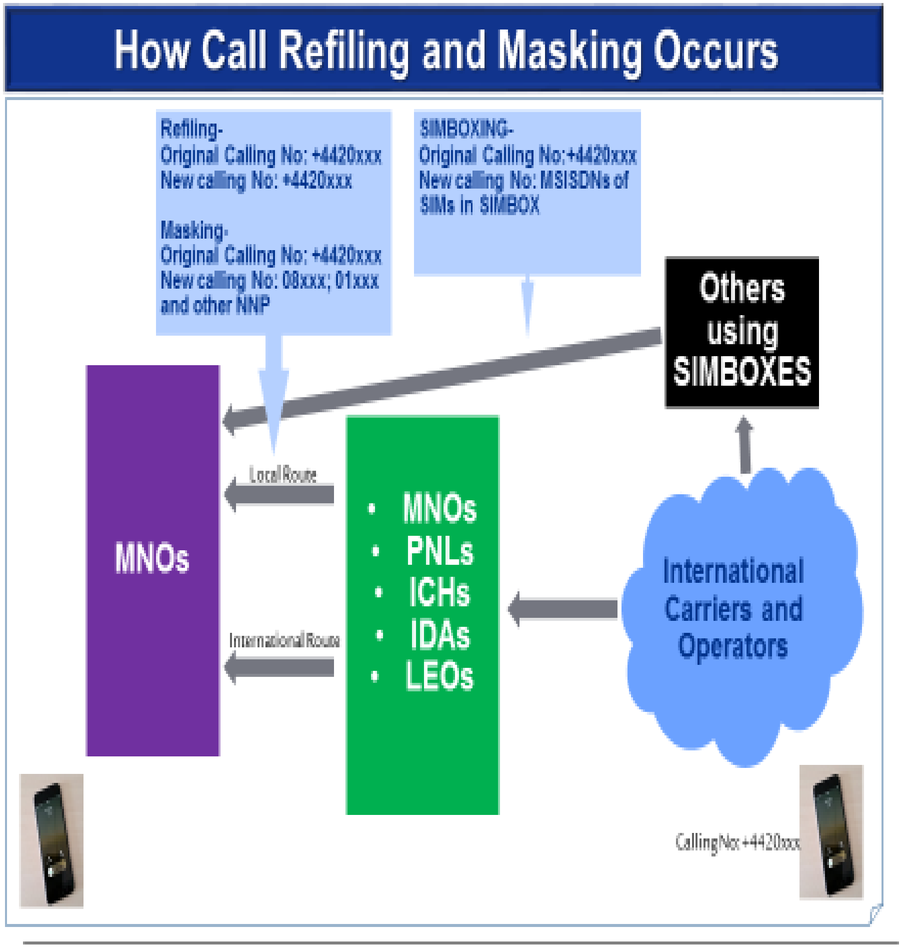
Deemed impermissible traffic



- Call Refiling & Masking
- Incoming unknown CLI
- Simbox
- OTT Bypass
- PRS
- Wangiri - International Call back
- SIM Swap & Cloning
- Spam Bulk SMS
- SMS Fishing

Call Refiling - Masking

- International calls are forwarded by an entity {originating} network to another entity (terminating network) using either the local interconnect means or international routes between the networks.
- This is usually done to exploit differences in [interconnection/ settlement] rates in order to achieve a cheaper interconnect.


How Call Refiling and Masking Occurs
Refiling-
Original Calling No: +4420xxx
New calling No: +4420xxx
Masking-
Original Calling No: +4420xxx
New calling No: 08xxx; 01xxx
and other NNP
SIMBOXING-
Original Calling No:+4420xxx
New calling No: MSISDNs of
SIMs in SIMBOX
Others using SIMBOXES
MNOs
Local Route
International Route
MNOs
PNLs
ICHs
IDAs
LEOs
International Carriers and Operators
Calling No: +4420xxx

Incoming unknown CLI

- Receiving international calls which appears in many cases as unknown calls
- As the Customer can’t recognize who is calling him or from which country the call is coming from.
- By imposing regulation on mobile operators to modify interconnection agreements to drop all unknown or undefined CLI which coming from international calls and replace it with the country code which the call is originated from, may help the customer to choose wither to accept or reject the call and also gives the customer least information about the caller.

Generally actual PSTN/PLMN numbers are used by different service providers or service aggregators while contacting their customers and partners. For example, taxi service aggregators like UBER or food delivery service providers use services of intermediaries like taxi drivers and food delivery agents.

Positive Impact

The impact of this method of communication by service providers decreases the possibility fraud call

Negative Impact

When service providers and operators are both involved in the call setup, the division of responsibilities becomes complex and unclear. Any misuse of call masking may lead to harassment calls or fraud calls

Sim Box

- Device used as part of a VoIP gateway installation.
- A SIM box can have SIM cards of different mobile operators installed
- Sim box international traffic entering the SIMBOX with a different CLI to exit the SIMBOX as a local CLI [traffic by the call taking the CLI (MSISDN) of one of the local SIMs in the box.]
- A Sim box is one way of achieving call masking in a voice call

• Interconnect Bypass Fraud

- Interconnect bypass fraud takes advantage of something called a termination rate to make cheaper phone calls.
- It costs telecom operators a huge revenue loss.
- Telco fraud experts use SIM cards from a local carrier and reroute international calls using a SIM box or GSM gateway.
- They are essentially making long-distance calls much cheaper for the callers and taking money out of the pockets of telco operators.

OTT Bypass

- An OTT bypass is where the call originates on a PSTN/PLMN network but is redirected and terminated on a mobile device via an OTT application without the knowledge or consent of the involved parties.
- OTT bypass is not the same as using OTT applications over MNOs’ data networks or using VoIP applications that permissibly interconnect with the PSTN.
- the originated calls to mobile numbers are redirected (mostly at the interconnect phase of call connection) towards the wholesale network, which in turn terminates the calls to OTT applications.
- This is usually facilitated as a result of OTT applications being linked to the mobile user through a MSISDN (commonly denominated mobile number).
- OTT bypass is totally different from using OTT applications over MNOs’ data networks.

• PRS

- Fraud occur due to commercial agreement gaps between some fraudulent carriers and operators which generate a huge traffic to PRS services and huge profit to the countries.

- Fraudsters can use auto- dialer equipment that is hidden in telephone or other telecommunications equipment. It is programmed to dial the PRS number and generate calls, often a large volume of short duration calls. Alternatively, or in addition, money is made by generating calls to a PRS number through deception. PRS owner makes large profits at the expense of the operator who fails to collect payment for the service.

• Wingiri - International Call back

- short calls Generated with the purpose of leaving a missed call notification on the Display of customers' handsets or a message is send to the customer thus prompting them to call back. The number displayed is a Premium Rate Service and the Call-back ensures artificial inflation of traffic.

• SIM swap - SIM cloning :

- Fraudsters may obtain a duplicate (SIM) card (including E-SIM) for the registered mobile number linked to the customer's bank account by gaining access to the customer's SIM card”.
- Fraudsters use the OTP received on such duplicate SIM to carry out unauthorized transactions. Fraudsters generally collect the personal / identity details from the customer by posing as a telephone / mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or 4G to 5G to provide additional benefits on the SIM card.

• Spam messages in bulk:

•Frauds due to the use of unknown/unverified mobile apps: fraudsters circulate through SMS, email, social media, Instant Messenger, etc., certain app links, masked to appear similar to the existing apps of authorized entities. Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer’s mobile, laptop, desktop, etc.

- Once the malicious application is downloaded, the fraudster gains complete access to the customer’s device. These include confidential details stored on the device and .messages / OTPs received before / after installation of such apps.

• Smishing/ SMS Phishing:

- Smishing, also known as SMS Phishing, is the practice of sending mass SMS in order to obtain personal information from the person who receives the messages.
- Mass spam campaigns are the bane of customers and telco’s existence. This is why SMS phishing rings have become adept at avoiding detection.
- They’ve been known to use software to confirm the numbers they target are mobiles
- create auto-shops to resell the stolen details, and even provide their own hosting services to host phishing sites and marketplaces.

SMS Sender ID Spoofing:

- Sender ID spoofing is a new type of spoofing that customer suffers from, as the customer will receive the SMS in the same thread that he has “ the same name of the Banking sender ID”, which will ease the fraudulent to gain any information from the customer wither by sending him a link or any other fake information.
- victims received an SMS from scammers claiming there were problems with their credit cards or accounts. The text message came in the same SMS thread as legitimate ones that the bank had previously sent, and it contained a link to a fake website imitating the bank. This conned a lot of clients.

• Sender ID Spoofing technical Solution:

- Blocking incoming international SMS traffic with alphanumeric Sender IDs that are not officially routed through licensed SMS aggregators.
- Register companies SMS Sender IDs, or the names that appears on customer messages, with national authorities so it might thwart illegal attempts by fraudulent.
- Develop a platform or an application that allowing organisations like banks to share phone numbers and malicious URLs that they have detected.