Use of SIM Boxes to bypass interconnect communications

Version 1.1

21 April 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

SIM Boxes (also known as GSM Gateways), are used to bypass the regular interconnect traffic towards mobile operators affecting the quality that customers experience. SIM Boxes have a major impact on the network quality, perceived by end-customers and on the traffic flows of mobile operators for termination of international traffic.

Mobile operators in different countries worldwide still suffer from high amounts of bypassed calls. In certain countries where mobile operators are taking actions against this issue for many years, the problem is under control. While in other countries, bypass issues are still increasing. Although the GSM Association has given a lot of attention in the past years towards SIM Boxes and SIM Box Detection, it needs to be noted that the problem is still highly affecting mobile networks, and only with rapid action of the mobile operators against SIM Boxes, the issues can be challenged.

In this document, GSMA defines the different forms of bypass via SIM Boxes. The impact SIM Boxes have on the traffic flows of mobile operators for termination of international traffic, the radio and network planning of mobile operators, as well as the quality degradations consumers perceive are presented. The document continues with a description of the mechanisms to detect SIM Boxes and some information on the evolutions in bypassing.

The figures and charts in this document are examples and for presentation purposes only.

> **Note**: There is an IMQ General Document available that presents the Business Case for implementing the prevention of the GSMA Gateways abuse (SIM boxes): IMQ Gen Doc 005.

2 Description of SIM Boxes

2.1 Introduction – Original purpose of GSM Gateways (SIM Boxes)

GSM Gateways are devices whose original purpose was to allow fixed line telephones to interface with mobile networks. The purpose is to provide fix telephone coverage in areas where no fixed coverage is available or in areas with temporary capacity problems due to different reasons (temporary headquarters, buildings construction, special events, and so on). The fixed line telephones are connected to the device that contains one or more SIMs. The SIM Box then connects calls made by the fixed line telephones to the GSM network using the SIMs contained within. Today SIM Boxes can interface via VoIP, PRI, fixed line, E1 and other means to collect the incoming traffic.

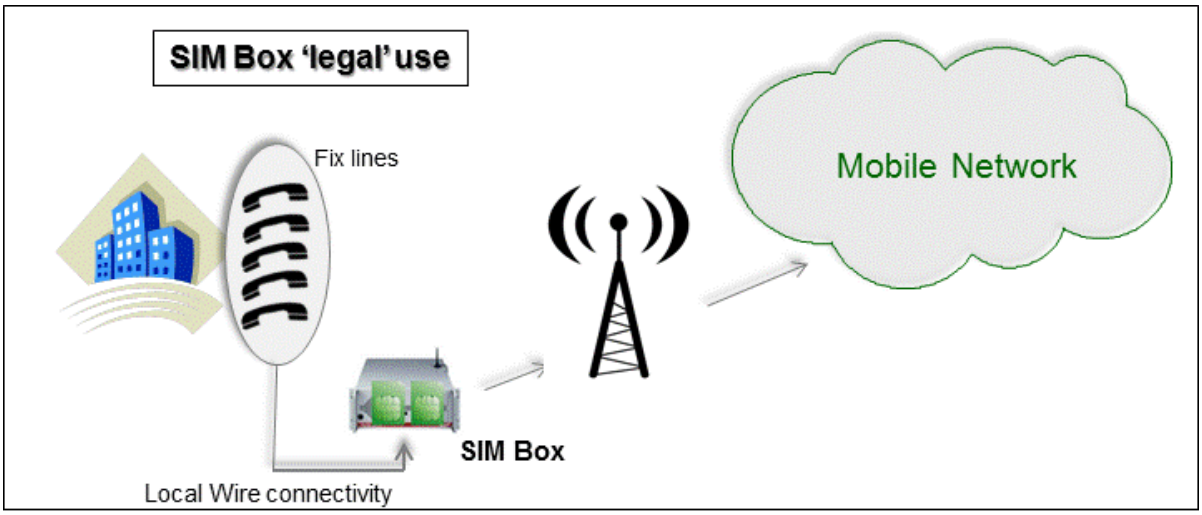

Figure 1: Sim Box legal use

Standard call routing between networks is shown in the figure below. This is the classical way of transmitting calls that maximises network efficiencies and call quality through industry standardised interfaces and processes. It is also consistent with standard international and national regulatory obligations relating to network interconnection.

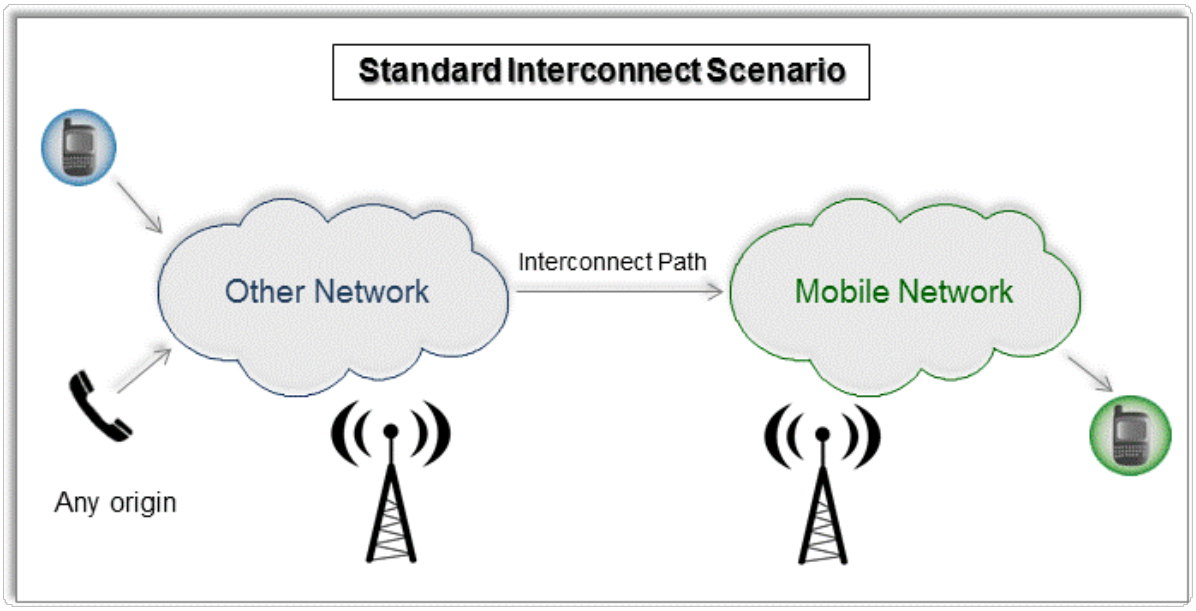

Figure 2: Interconnect Scenario

The set-up of calls via a SIM Box is shown below. In this case, calls from another network are made to appear as mobile-to-mobile calls on the GSM network. This is likely to create significant quality issues for mobile networks. Especially since such arrangements are established without the prior knowledge of the mobile network operator.

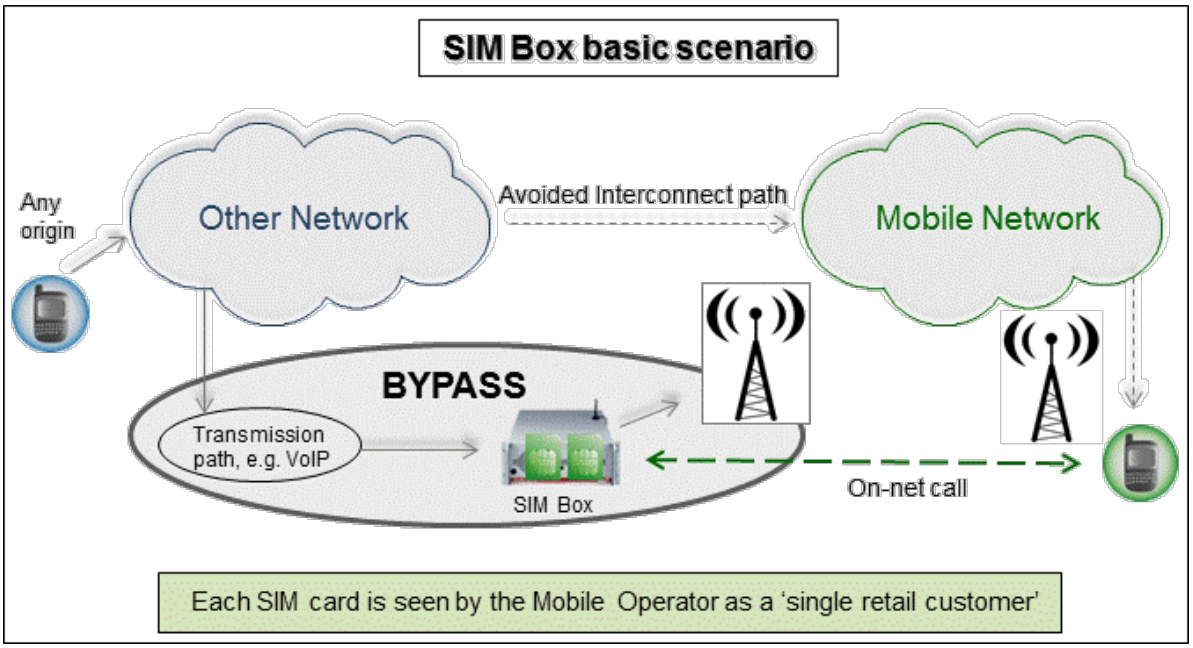

Figure 3: Sim Box basic scenrio

Some networks allow corporate customers this type of access to provide direct connection with the customer's private network, creating a sort of virtual private network (**Note**: corporate customers do not have an Operator's Licence and may not be able to ask for Interconnection to the mobile network). In such cases, services are normally restricted to closed user groups under the control and knowledge of the mobile operators. Due to these restrictions, quality losses are minimised.

However, SIM Boxes are increasingly being used by national and international voice carriers via third parties or re-sellers, to bypass traffic. These may not have an operator's licence to route calls to GSM networks or even use subscription fraud.

Some vendors of GSM Gateway equipment are now specialised in the equipment used for this kind of bypass traffic, in order to optimize the use of SIM Boxes worldwide. More information about the specific features of these installations can be found under Chapter 8.

Mobile operators are unaware of the deployment of such SIM Boxes, resulting in unpredicted network behaviour and quality problems. With this type of connection, customers may be denied the normal industry standard quality guarantees expected of public networks.

2.2 On-net Bypass

Bypassers use the best on-net retail calling rates (for example promotions to attract new customers) to terminate calls via a SIM Box instead of via the regular interconnect. The way a bypasser uses these local promotions to terminate international traffic is illustrated in following example:

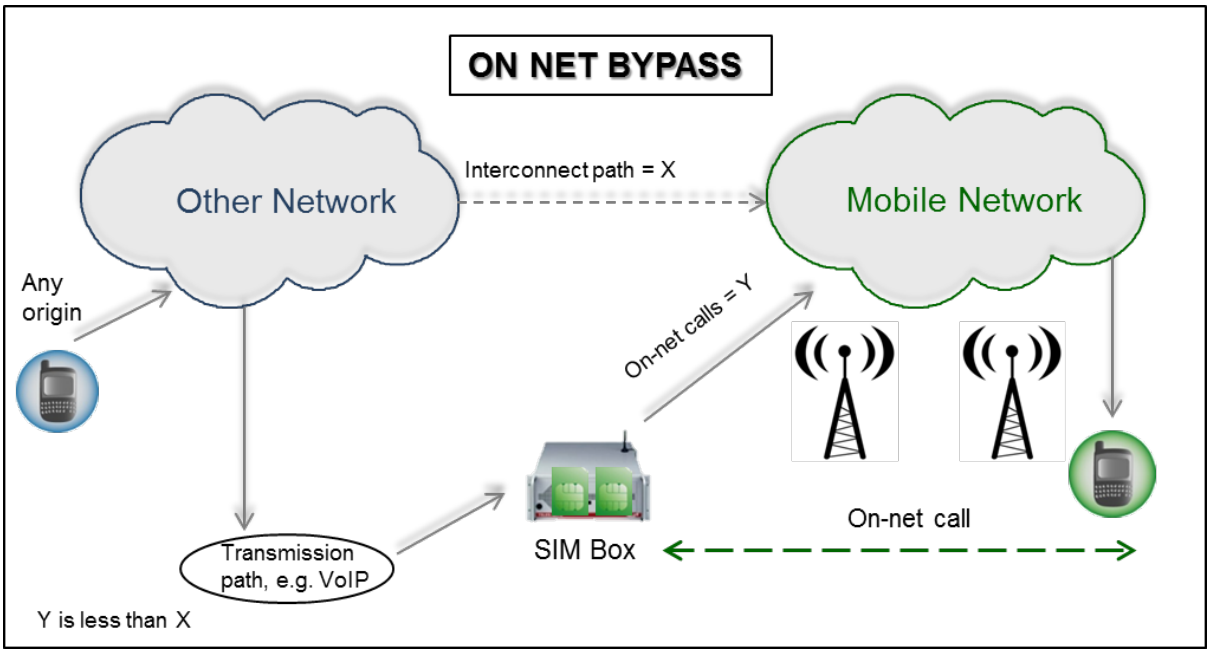

Figure 4: Bypass On Net

In the above example, the rate for termination of international traffic equals X. The *other network* on the left, is sending the traffic via an alternative interconnect path, namely a SIM Box towards the *mobile network* (the SIM Boxer will stay anonymous, so the *other network* will often send the traffic through a third party, without the knowledge that it is a SIM Box).

If traffic is sent via the alternative path, it looks for the mobile operator like two regular customers are making an on-net local call on his network. Instead of X, the International Termination Rate, the applicable rate will by Y. (Y equals a local tariff, subject to specific promotions and conditions that are applicable to the retail market, not to the interconnect market).

If SIM Boxes are in operation, a shift occurs from minutes terminating at the termination rate for international traffic (X) to minutes at on-net retail tariffs (Y). The charge per minute for on-net calls will by definition be lower than the termination rate (Y is less than X) otherwise the SIM Box phenomenon would not occur.

2.3 Off-net Bypass

In a number of cases, mobile operators have tariff plans that offer low rates to all mobile operators of the country, on-net and off-net. In case this rate is lower than the interconnect rate for one or more other mobile operators, SIM Cards of one operator might be used to terminate calls to other operators also. The way this set up is organized by a bypasser is illustrated in the following example:

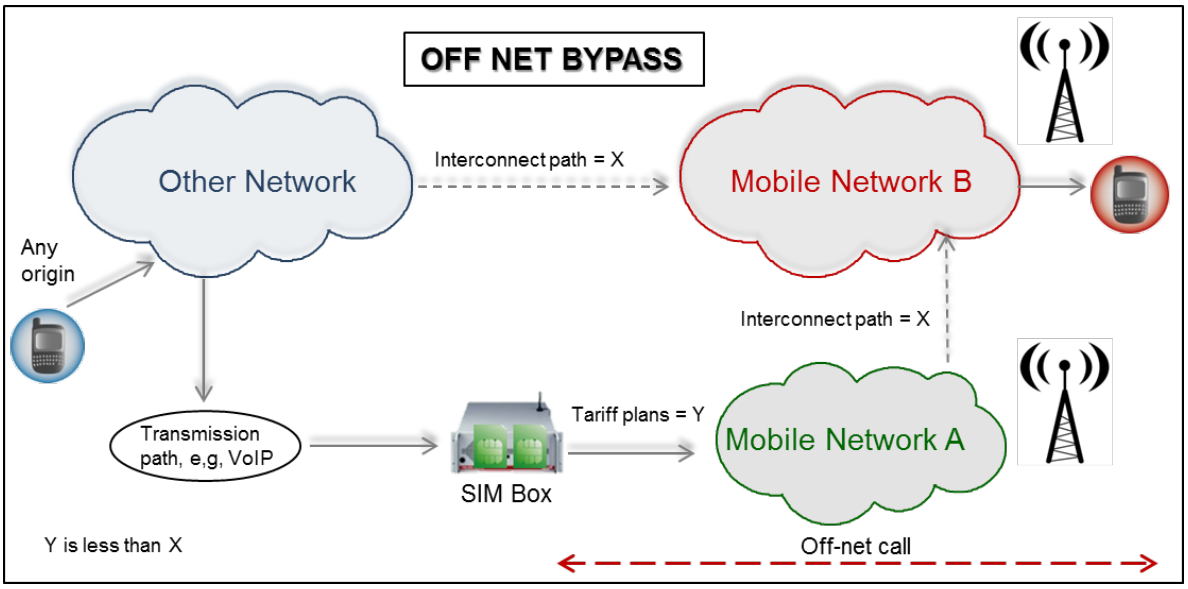

Figure 5: Bypass Off Net

In the above example, the rate for termination of international traffic equals X. The *other network* on the left, is sending the traffic via an alternative interconnect path, namely a SIM Box towards the *mobile network B*.

The SIM Boxer terminates the call via tariff plan Y, on the *Mobile Network B* (Y equals a local tariff, subject to specific promotions and conditions that are applicable to the retail market between customers of A and B, not to the interconnect market). For network A, it looks like a regular customer is making a call from his network towards network B. Mobile network A only receives Y via the local tariff plan, while Network A has to pay X towards Network B.

2.4 Leaky PBX

A Leaky PBX follows the same principle as a SIM Box but instead of a SIM card, the bypassers use a fixed line to terminate the traffic. Leaky PBX operators use the difference between the lowest fixed to mobile tariff and the interconnect rates. In some cases the corporate PBX's are used for this purpose. Leaky PBX exists in both forms on-net and off-net. The on-net form is illustrated in following example:

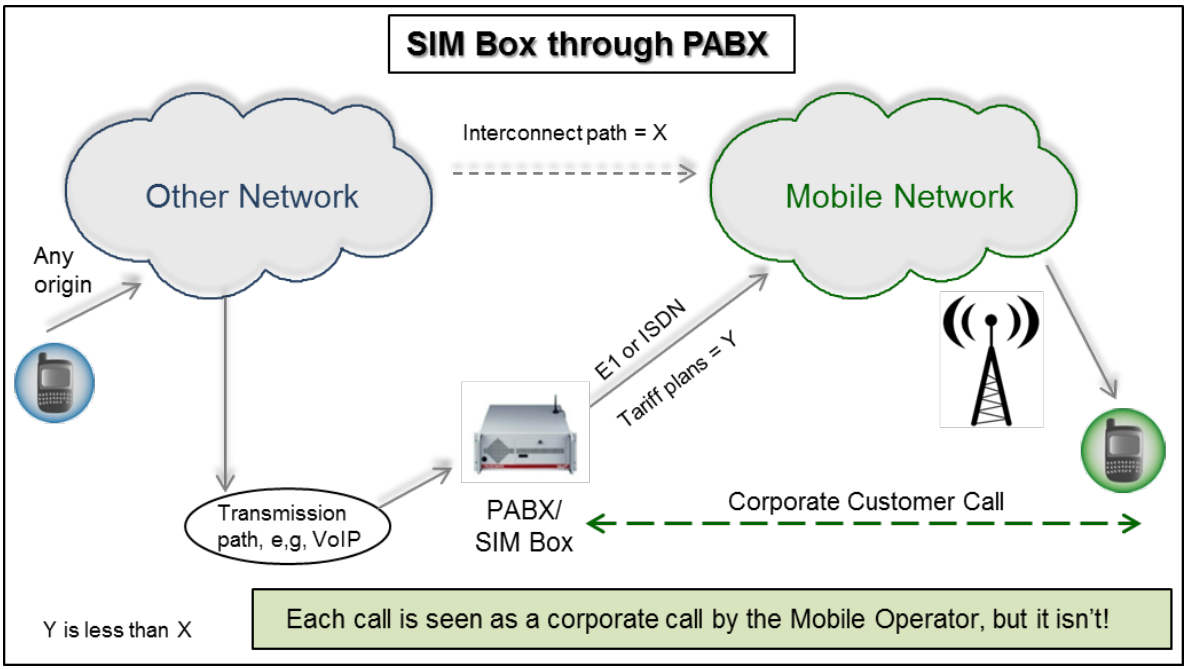

Figure 6: Sim Box through PABX

In the above example, the rate for termination of international traffic equals X. The *Other Network* on the left, is sending traffic via an alternative interconnect path, namely a Leaky PBX, towards the *mobile network*.

The Leaky PBX terminates the call on the *mobile network* via a local tariff plan. Instead of the regular rate for termination of international traffic, X, the mobile operator only receives Y from the local call at a local tariff plan.

The quality issues due to the use of an extra radio channel explained in the following chapters are not valid in this case. However, remarks on lower voice quality, unsuccessful calls and longer call setup times remain applicable due to the extra PBX interface. Please note it is possible to spoof the CLI (Calling Line Identity) with a PBX (in case it is permitted by the fixed network).

2.5 International Off-net Bypass

The globalized telecommunications market and increased competition forced operators to become more creative in creating retail tariffs plans that are offered to customers. Some operators introduced a low cost or even flat rate tariffs towards some international destinations that could be lower than the international termination rate (retail rate < international termination rate of a particular country). This might be used to terminate calls to other networks, as illustrated in the following example:

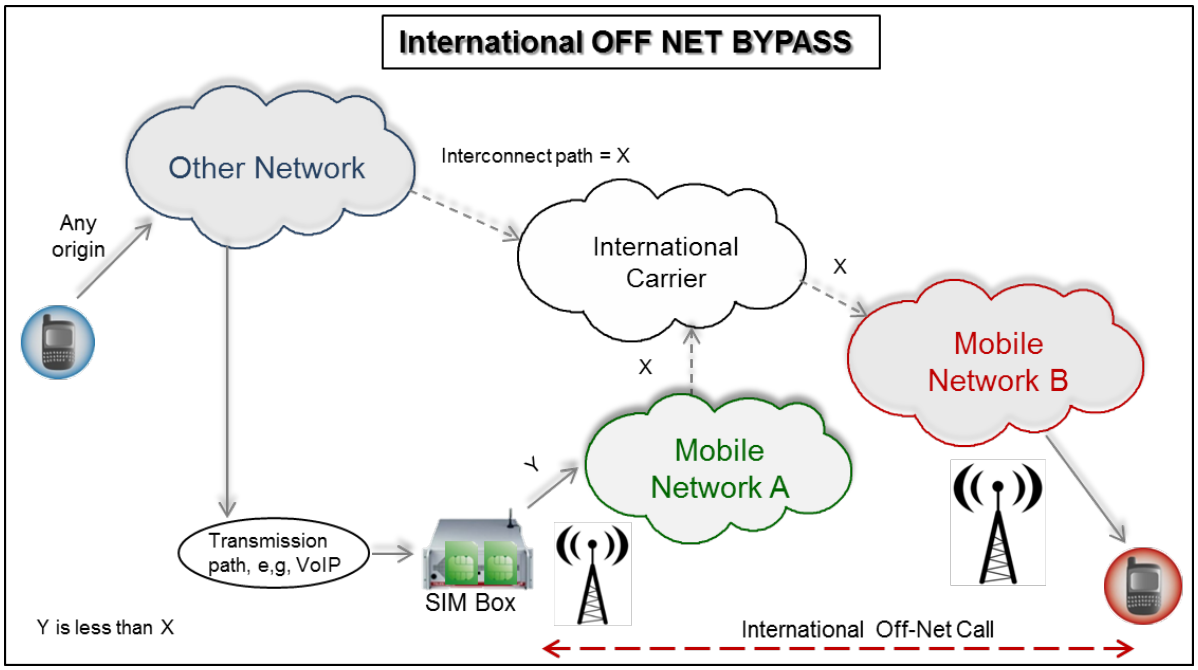

Figure 7: Bypass International Off Net

The impact on Mobile Network A and Mobile Network B is comparable to the national off-net bypass scenario.

Mobile network A receives Y via the local tariff plan, while Network A has to pay X towards the next interconnect partner, in which case Y is less than X.

As a result of the diverted call via a SIM Box, the customers of Mobile Network B will suffer quality losses. The impact on the quality for end customers is explained in detail under paragraph 4.

2.6 SMS bypass scenario

In addition to bypassing voice traffic, SMS traffic can be bypassed via different methods.

For more information regarding the different fraud scenarios and measures that can be taken by mobile operators to reduce their level of exposure we refer to the following documents:

- IR.70 SMS SS7 Fraud
- IR.71 SMS SS7 Fraud prevention
- FF 09 Introduction to SMS Fraud

3 Impact on Radio and Network Planning

3.1 Inefficiency of Radio planning

The use of SIM Boxes significantly reduces bandwidth efficiency, as a SIM Box uses two radio channels for mobile to mobile calls, while normally only one radio channel is required. Using additional radio resources, where it is not required, may be inconsistent with statutory duties of radio authorities.

3.2 Network Planning and Operation

SIM Boxes are fixed and contain large quantities of SIM cards making large volumes of calls. The network therefore experiences abnormally high demand on individual cells, causing network congestion. Cell sizes are becoming very small in the areas where SIM Boxes are located. High concentrations of users may be unsupportable as it is likely to be impossible to shrink cell sizes any further and add additional infrastructure (capacity). Therefore, **mobile users can be denied service**, particularly since SIM Boxes often 'grab' the available cell capacity from early in the morning until late at night.

4 Consumer Impact

4.1 Detriment Due to Non-delivery of Signalling Data

Bypassed calls via SIM Boxes do not allow the delivery of the correct and original CLI of the calling party. This results in consumers being unable to use services that they would expect to be able to use. These services include:

- Returning a missed call through voice or SMS
- Screening unwanted or malicious calls
- Using an anonymous call rejection system (if offered by the operator)
- Managing roaming costs (customers may use CLI to decide whether to accept the call)
- Other CLI based services offered by the operator, such as: seamless access to voice mail, the development of a virtual home environment, and in general the roll out of all services based on an authentication of the customer and cross reference to network databases
- Voice mail retrieval when roaming abroad (direct or via short code)
- Voice mail deposit when roaming abroad

These limitations need to be considered against regulatory and industry guidelines for the delivery of CLI. Furthermore, there is legislation concerning the processing of personal data and the protection of privacy in the electronic communications sector dealing with calling CLI. In line with this legislation there are certain obligations on service providers regarding the provision of CLI.

It is GSMA's view that SIM Boxes compromise the integrity of CLI and as a result, service providers may not be able to fulfil their regulatory obligations in this regard.

4.2 Inbound roamers not reachable

Customers roaming on foreign networks may be unable to receive calls if incoming calls have been routed via a SIM Box. Retail SIM Cards are prohibited to phone the MSRN directly due to network security basics, which results in unreachable inbound roamers.

This is illustrated with the following example:

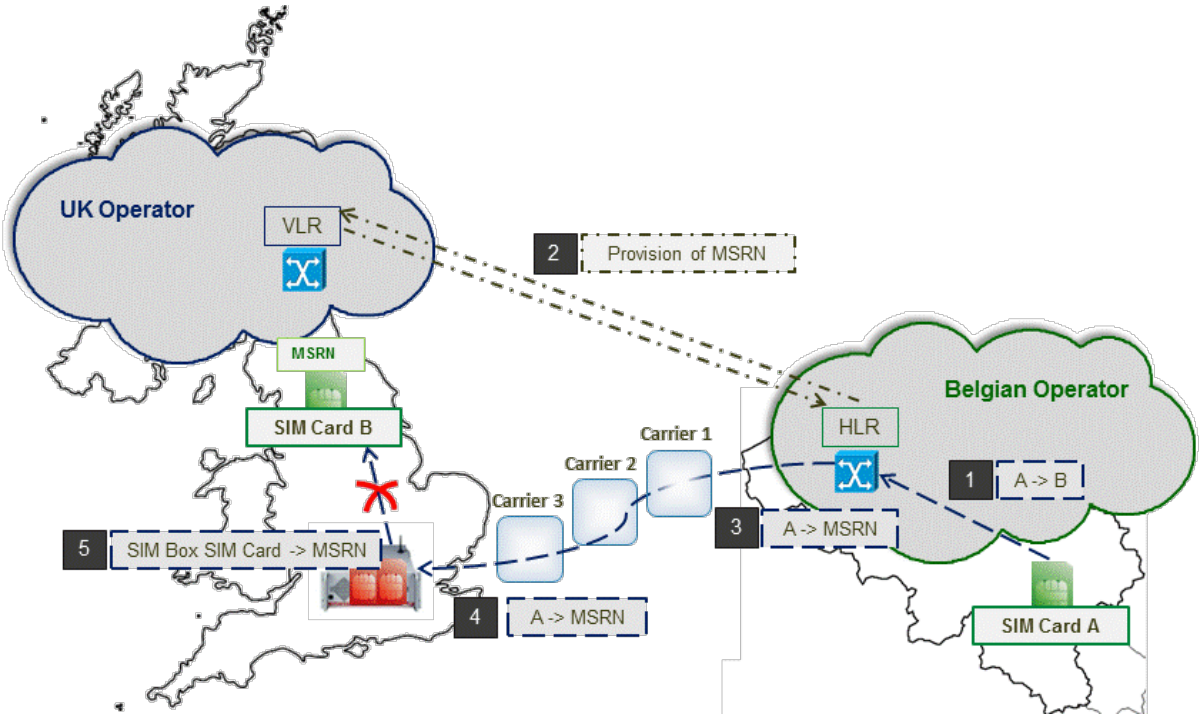

Figure 8: Sim Box use: Inbound roamers not reachable

Description:

- **Step 1: A calls B (A -> B):** SIM Card A is calling SIM Card B (dialling the MSISDN associated with the SIM Card B).
- **Step 2: Obtaining MSRN:** As SIM Card B is roaming in UK, the Belgian operator needs to ask for a visited network' MSRN in order to route the call to the visited network.
- **Step 3: Normal international routing A calls MSRN (A->MSRN):** the Belgian mobile operator routes the call (UK MSISDN belonging to the visited operator) through their selected carrier.
- **Step 4: Bypassing the regular interconnect routes:** The last carrier in the interconnect path passes the call via a SIMBoxer instead of using the regular interconnection with the UK visited operator.
- **Step 5: SIM Box calls MSRN (SIM Box SIM Card -> MSRN):** The SIMBoxer tries to set up a call to reach the MSRN but the UK network will not allow the call due to network security; a retail SIM card from the visited operator is not able to call to the same operator MSRN directly. By this way, SIM Card B is not able to receive an international call if this call is routed via a SIM Box.

4.3 Service Disturbance

Customers may not be able to establish a call (or an existing live call may be terminated) if this call passes through a SIM Box using prepaid SIMs which are not recharged in real time. In case a prepaid SIM card in a SIM Box is out of credit, the calling party from abroad, may receive the following network message: *"Your account balance doesn't allow the call completion"* There is no sense in receiving this message for post-paid customers.

In addition, quality issues can arise when customers try to use certain supplementary services while SIM Boxes do not support this service. A good example is video telephony, which will never reach its destination because SIM Boxes were not configured or do not support that type of service. The same issue applies with fax and circuit switch data.

Mobile operators cannot control the above-mentioned situations and are subjected to high levels of complaints, churn, diminished service reputation in the market and customer requests for financial credits (for example: a customer being unable to conduct business while abroad, and so on).

This seriously affects the reputation of GSM mobile networks and the service quality experienced by users (which may also affect the operators' ability to satisfy license obligations).

4.4 Ability of mobile customers near SIM Boxes to make or receive calls

The use of SIM Boxes on mobile networks will have an adverse impact on customers' experiences as the excessive demand placed by SIM Boxes on certain cells will result in poor network coverage in some areas. Mobile customers may be unable to make or receive calls during the hours when SIM Boxes operate at full capacity and use all, or nearly all, of the cell capacity.

This will also affect the operators' ability to fulfil its obligations in respect of emergency calling.

4.5 Lost Calls and Call Routing Problems

Interconnection capacity is monitored and adjusted according to the utilisation levels and the availability of overflow routes. In case of usage of SIM Boxes, this monitoring cannot take place, resulting in congestion due to bypass, which results in the loss of calls. Calls to mobile subscribers can also fail under certain call scenarios where the called subscriber is roaming or where the called number has been ported to another network within a country where a mobile portability solution has been adopted. This damages the customer experience and makes it difficult for network operators to identify the causes of such call failures.

4.6 Increased Call Set-up Time

Due to the call set-up process of SIM Boxes, the post dial delay will significantly increase. In most cases the customer is unaware that the call is being routed through a SIM Box, resulting in an incorrect perception of poor network quality. The originating network, the international voice carrier and the terminating network, can be affected by these perceptions, resulting in loss of reputation for any of them.

In addition, a long call setup time will decrease the usage of consumers of their handset, resulting in lost calls due to quality issues.

Furthermore, it is significant to highlight the importance of long call set-up time on emergency calling.

Finally there are some countries where the quality standards promoted by Governments may be by-passed and cause penalties.

4.7 Deterioration in Voice Quality

In general, cellular voice quality is very good. In the case of SIM Boxes however, the well-known transmission difficulties of the radio environment are likely to cause an increase in dropped calls and noise. This is an undesirable consequence to both the called and calling parties. The reason therefore is that due to the use of SIM Boxes, two radio legs rather than one are involved. Again, this will have an impact on emergency calling.

4.8 Privacy Issues

If a call is routed through a SIM Box it may tumble upon the SIM Box's SIM voicemail. As the calling consumer believes he has reached the voicemail of the requested destination number, he may leave a confidential message on that SIM Box's SIM voicemail.

5 License obligations and other legal issues

In cases where calls are routed via SIM Boxes, the CLI of the originating party is not transferred and the called party will receive the CLI of the SIM card that is used in the SIM Box.

Most operators have licence obligations to co-operate with the law enforcement agencies who have the authority to request identification and monitoring of mobile traffic (using the GSM MSISDN number/CLI). When there is use of SIM Boxes without the Mobile operator's knowledge and permission then the real CLI of the originating party is not known. Therefore, the mobile operators cannot fulfil these obligations. In some cases (for example in Belgium) the police authorities have already contacted mobile operators requesting clarification of this problem.

The absence of a correct CLI also prevents an operator from detecting the origin of malicious calls and thus prevents helping the affected consumers. Finally, the incorrect CLI compromises the correct handling of emergency calls (normally a licence obligation) where CLI is used to detect the victim's location. This is a subject of general interest where the mobile operator cannot take up his responsibilities of 'good corporate citizenship'.

6 Fraudulent Revenue Losses Caused by SIM Boxes

6.1 Service Revenue

These are indirect revenue losses caused by the service disturbances & customer dissatisfaction as described in chapter 4 of this document.

6.2 Radio Investment

Some SIM Boxes use more than 32 SIMs simultaneously at one location. Operators may need to install extra radio equipment or even new antenna sites only to compensate for the SIM Boxes, leading to large investments merely to generate quality, revenue and service disturbances.

6.3 Cost of Sales

Fabrication and distribution of SIM cards to be used in SIM Boxes to bypass traffic (and thus generate revenue losses), costs money. In some cases (for low credit pre-paid cards) the SIMs are thrown away within 30 minutes.

7 Mechanisms to Detect SIM Boxes

7.1 Manual testing

This mechanism is reflected on each IR21 test numbers database and consists on a simple test call for numbers which can only be accessed from the “true” Network-to-Network interface, and which cannot be accessed from a mobile station.

These test number are made available by IREG and therefore by all PLMN, through a directory number on Auto-Answer Circuits. It is suggested that these number could be from fragments of a range used for MSRNs and HONs (Hand-over Numbers), but not actually assigned to a particular MSC.

As mentioned, these numbers cannot be accessed from a Mobile Station, but is accessible from genuine Network-to-Network interconnection points only. Therefore provides carriers with an easy test so that they can check to see if a downstream carrier is using a SIM Box device.

This procedure is described in GSMA document IR.21. More information about manual testing and the comparison with other detection mechanisms can be found in IN.22.

7.2 Passive detection

Mobile operators can detect SIM Boxes by using multiple criteria on traffic & customer data. These are some examples of common criteria to trigger bypass alarms:

- Only outgoing calls
- No SMS
- No GPRS
- High volume of traffic
- Small company but high call costs
- Suddenly lots more traffic in one antenna cell
- All calls from the same antenna cell
- SIMs using a blacklisted IMEI
- Activation of a lot of pre-paid SIMs without using them immediately

Operators can develop an in-house solution or use one of the fraud management systems available on the market.

7.3 Active detection

These detection systems actively set up international calls and compare the CDR created on both sides to detect SIM Boxes. A-side can be fixed, mobile, VoIP, calling card, carrier, call back and so on. There are multiple solutions available on the market.

In the selection of an active detection system, mobile operators should be aware that the active detection system supports countermeasures, in order to avoid detection of the test calls by SIM Box operators.

In case the active detection system does not support countermeasures, there is a high possibility that SIM Box operators will soon discover the calls made for test purposes and

avoid being detected. More information on advanced SIM Box bypassing can be found under Chapter 8.

7.4 Combination of detection mechanisms

It should be noted that both an active detection system and a passive detection system can be used in combination. Often the results of an active detection system can be used and extrapolated to feed the internal passive detection system of a Mobile operator.

8 Evolutions in SIM Box bypassing

The equipment and software, used for bypassing the regular interconnect has seriously evolved in the last few years. In this paragraph, we define some of the most important features SIM Box operators make use of during their activities.

8.1 Human behaviour simulation

SIM Boxes can simulate human behaviour in order to avoid being detected by mobile operators. Therefore, they will ensure their call behaviour is not suspicious.

Some examples of human behaviour simulation are the following:

- Each SIM card in the SIM Box is only used for a few hours per day. Multiple SIM cards are used and often switched, in order to ensure normal call patterns;
- Free minutes are used to phone from SIM card to SIM card within the SIM Box. In this way, the call behaviour of the SIM cards is not limited to outgoing calls only;
- Free SMSs are used to send SMS towards the SIM cards in the SIM Box. In this way, not only voice services are used.

8.2 Automatic SIM replacement

SIMs are automatically rotated, for example, once their prepaid credit is zero.

8.3 Moving equipment

Bypassers are known to move their equipment. Changing antenna cell simulates human behaviour.

8.4 Multiplexers

Some bypass operators have multiple SIM Boxes at different locations, but only one centralized storage point for the SIMs. They use multiplexers to virtually copy the SIMs to the SIM Box equipment. This avoids the need of a human presence in each SIM Box location, and allows moving SIMs to another antenna regularly.

8.5 Time Windows

SIM Boxes can use a different selection of SIMs during peak and off-peak hours, week and weekend. The choice of SIM cards used during certain time frames depends on the promotion of that moment. By using specific software, SIM Box operators have the possibility to manage the timeslots per SIM card. Via this optimal usage of promotions, profits can be maximized.

8.6 New IMEI send with every new SIM card/call

Advanced SIM Box equipment provides the SIM Box operator with the possibility to spoof the IMEI (International Mobile Equipment Identity) of the SIM Box equipment. By this way, some SIM Box operators send a different IMEI for every SIM card used and sometimes even for every call made. Meaning, the mobile operator is not able to extrapolate the results of the detection of one SIM, to block all SIMs with that same IMEI number. Invisible customer

Bypassers may use third parties or multiple people to buy the SIMs, making it nearly impossible to identify SIM Boxes through customer profiling.

8.7 Subscription Fraud

Some SIM Boxers maximize their profits by using SIMs purchased with false IDs, cloned SIMs, stolen SIMs, and so on. In certain countries fraud and criminality are closely linked with interconnect bypass.

9 Summary and Recommendations

For the reasons outlined in this document, mobile operators should be concerned about the congestion, quality and user experience impairments associated with the use of SIM Boxes. This particularly applies to the uncontrolled use by carriers where mobile operators may have no prior knowledge and have to make unpredictable network planning and optimisation changes.

A first possibility being implemented by most operators is to ensure that **commercial terms and conditions exclude the use of SIM Boxes** for routing third party traffic. Operators should then also be free to detect, identify and terminate such subscriptions which are in breach of contract or in breach of any national legislation preventing the use of such devices.

Mobile operators should be free to define reasonable commercial terms and conditions to protect the integrity and quality of their networks.

It is possible that to disincentive the use of SIM Boxes, mobile operators could explicitly exclude the use of unauthorized SIM Boxes (different from private and corporate users) from special traffic discounts given to their customers.

Mobile operators can also sign Roaming Service Level Agreement's (RSLA). Further information about RSLAs are described in BA.51. Both Roaming and Interconnection departments should work closely to prevent Gateway bypass, as this interconnect scheme reduces roaming and international interworking quality.

Furthermore, National Regulatory Authorities (NRA) may promote the interests of the citizens by ensuring that the integrity and security of public communications networks are maintained. It is argued that the use of SIM Boxes compromises the integrity and security of our members' networks and as a result our members' regulatory obligations may be called into question by the relevant NRA.

Customer Care Impacts should be taken into consideration in the detection method of SIM Boxes. **The operator must ensure an MSISDN is not identified incorrectly as a SIM Box**, irrespective of the detection method applied.

Operators must foresee procedures to ensure customers are refunded for damage caused in case their MSISDN has been deactivated incorrectly.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	30 Jan 2015	New PRD FSG.01 derived from IN.02 v5.2	Fraud and Security Group	Nick Cheung (GSMA)
1.1	21 Apr 2023	Updated GSMA logo	N/A	David Maxwell (GSMA)

Other Information

Type	Description
Document Owner	FASG
Editor / Company	David Maxwell (GSMA)

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.