COMBATING NON-COMPLIANT DEVICES

TYPE APPROVAL (SIM ENABLED DEVICES) VERIFICATION

CONSULTATIVE PAPER

NOVEMBER 2020

TABLE OF CONTENTS

ACRONYMS

BOCRA	Botswana Communications Regulatory Authority
CRA Act	Communications Regulatory Authority Act
EIR	Equipment Identity Register
EMF	Electromagnetic Field
CEIR	Central Equipment Identity Register
GSMA	Global System for Mobile Communication Association
IMEI	International Mobile Equipment Identity (IMEI)
IMSI	The international mobile subscriber identity
ITU	International Telecommunication Union
TAC	Type Allocation Code
TRIPS	Trade-Related Aspects of Intellectual Property Rights
WIPO	World Intellectual Property Organisation
WTDC	World Telecommunications Development Conference
WTSA	World Telecommunications Standardization Assembly
WTO	World Trade Organization

1. INTRODUCTION

1.1. In pursuit of its mandate for the consumer protection and implementation of type approval requirements, BOCRA, (herein with, the Authority) is undertaking further measures to combat the proliferation of non-compliant devices which use telecommunications networks. Non-Compliant Devices include; counterfeit devices, non-type approved device and substandard devices. The measures under consideration include registration of devices before connected for use to the public networks.

1.2. Like most developing countries, Botswana has witnessed a proliferation of counterfeit/substandard devices on its ICT market during the past years. The rampant trade in counterfeit /substandard mobile devices including but not limited to the smart ICT accessories such as batteries, chargers, watches etc.

1.3. These have slowly eroded consumer confidence. As a result, it is difficult to ascertain if the said ICT devices and accessories are safe for public use and also have a potential to contribute to degraded quality of service.

1.4. In addition, the lack of rigorous border clearance and inspections when it comes to the importation of ICT devices and accessories indicates that government is unable to maximise its revenue collection via import duty and sale tax.

1.5. As technology develops rapidly, the mobile services grow and device penetration increase. This continued growth of mobile penetration to serve the increasingly vulnerable and socially

disadvantaged members of society mean the concerns of counterfeits devices continue to grow.

1.6. There are efforts made towards combating the proliferation of the said devices through public institutions for instance, Botswana Police, Ministry of Trade and Botswana Unified Revenue Services. However, these efforts have fallen short in many respects as criminal networks are quick to adapt their operations and spot loopholes to avoid and circumvent law enforcements.

2. OBJECTIVE

2.1. BOCRA intends to carry out consultations with stakeholders on possible ways to deal with non-compliant devices. This consultation paper aims to discuss the following: the

2.1.1. Impact of the counterfeit/substandard devices on the ICT ecosystem;

2.1.2. Regulatory challenges; and

2.1.3. Proposed regulatory Guidelines, technical solutions and strategic processes that could be implemented, i.e.

2.1.3.1. Type Approval (SIM Enabled Devices) Verification Guidelines;

2.1.3.2. Type Approval (SIM Enabled Devices) Verification System, and

2.1.3.3. Collaborative partnerships

3. THE CONSULTATIVE PROCESS

3.1. With this consultative process, the Authority seeks the contributions and comments from the public and stakeholders regarding the proposals contained in the following documents:

3.1.1. Annexure 1: The Draft Guidelines;

3.1.2. Annexure 2: Feedback Questions

4. BACKGROUND

4.1. The liberalization of the telecommunications market in 2008 and the further reductions in trade barriers has provided benefits for both businesses and consumers alike. However, this has also provided opportunity for illicit trade SIM Enabled devices.

4.2. The Authority has since proactively put the following measures to control the influx of non-compliant devices. These measures include;

4.2.1. The Type Approval Guidelines;

4.2.2. Regular market surveillance activities; and

4.2.3. Educational campaigns.

5. AVAILABLE REGULATORY INSTRUMENTS

5.1. Nationally, the Communications Regulatory Authority Act of 2012, in Section 84, empowers Authority to specify the type of equipment

connecting to the network and to type approve all communication equipment.

5.2. Regionally, the Communications Regulator of Southern Africa, (CRASA) has put in place guidance to assist the regional harmonization efforts to tackle proliferation of counterfeit devices.

5.3. Internationally, the International Telecommunications Union (ITU) is repository of the recommendations (standards) that discusses this subject matter through its structures as follows:

5.3.1. The ITU highest decision body, *the Plenipotentiary-14 Resolution 188 – Combating Counterfeits in Telecommunication and ICT Devices;*

5.3.2. World *Telecommunication Standardization Assembly, WTSA-16 Resolution 96 - Combating Counterfeit in Telecommunication and ICT Devices; and*

5.3.3. World *Telecommunication Development Conference, WTDC- 17 Resolution 79 - The role of ICTs in Combating and dealing with counterfeit and communication devices*.

6. THE DISCUSSIONS

6.1. WHAT ARE COUNTERFEITS?

6.1.1. The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement) defines counterfeit trademark goods as "any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of

such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation" (footnote 14 to Article 51).

6.1.2. These devices are used as a safe revenue stream by illegal supply networks and has proliferated with the rise of the Internet, which gives counterfeiters the reach to sell to consumers globally, outside the national limits of law enforcement.

6.2. WHAT ARE SUBSTANDARD DEVICES?

6.2.1. Although there is no ITU definition of Substandard ICT terminal, substandard is a category of ICT terminal that is sold in contravention of applicable national and international technical standards, conformity processes, as well as national regulatory requirements or other applicable legal requirements. In some cases, the manufacturer may intend to deceive the purchaser into believing that the device bought is compliant.

6.3. WHAT IS A NON-TYPE APPROVED DEVICE?

6.3.1. The Communications Regulatory Act Section 84 (2) specifies that; *A person who provides a telecommunications service or supplies telecommunications equipment shall not use any telecommunications equipment which has not been*

type approved by the Authority and no person shall connect, to any telecommunications system, any telecommunications equipment which has not been type approved.

6.3.2. A non-Type Approved device is the device that has not been taken through the Type Approval registration process and as such does not have a certificate to show it is BOCRA approved to be connected or used in Botswana networks. The Type Approval registration process defines the national compliance status of a device. Usually, the counterfeit and substandard devices are not taken through the Type Approval registration process.

6.3.3. It is still possible however that some legitimate devices are used in the networks because of negligence of suppliers to the type approval registration process.

7. THE IMPACT OF COUNTERFEIT ON THE ECOSYSTEM

7.1. The use of the counterfeit and sub-standards devices has several impacts either negatively or positively on the different elements of the communications ecosystem. The seemly positive impacts associated with the use of these devices may conceal the adverse negative effects. The effects create different results on the operations of the government, consumers, industry (operators, manufactures, resellers, retailers and distributors) and the environment. The details are outlined in the following paragraphs.

7.2. NEGATIVE IMPACTS

7.2.1. National Government

7.2.1.1. Tax and Duties are evaded by the counterfeiters and as such huge sums of money which would otherwise be earned by governments are denied through illegally bringing the devices through informal routes;

7.2.1.2. Furthermore, additional resources are used by government to counter these undesired activities;

7.2.1.3. Security and integrity on networks/national infrastructure are compromised when counterfeit devices are used;

7.2.1.4. The regulatory cost is inflated by the existence of the Counterfeits / substandard products as elaborated in the process above. More staff, man-hours and collaboration efforts are needed to just address these to safeguard the industry and assure Consumers of quality and protection from the associated harmful effects.

7.2.2. Consumers

7.2.2.1. They pose security vulnerabilities and threats to subscribers' privacy, criminal activities;

7.2.2.2. Naturally mobile devices contain hazardous substances which can be dangerous when not

properly disposed of (e-waste), on the contrary counterfeit devices pose a higher risk of containing unacceptable levels of such substances since they were not manufactured up to correct standards hence the risk to human health and safety;

7.2.2.3. Such devices can equally emit harmful EMF radiation during use by consumers;

7.2.2.4. Consumers are enticed to buy such devices because they cost less. This directly impacts the industry involved in the supply chain of genuine devices;

7.2.2.5. The devices have a shorter life span;

7.2.2.6. Quality of experience by the consumer is negatively affected, and

7.2.2.7. The devices may affect other devices operating within the vicinity.-

7.2.3. Network Operators

7.2.3.1. Potential degradation of the network performance resulting in overall decline in quality of service; and

7.2.3.2. Counterfeit devices often cause harmful radio interference.

7.2.4. Manufacturers

7.2.4.1. Manufacturers of original devices invest heavily in developing their products, only for these devices to

get to the market and compete with the counterfeit/substandard devices; and

7.2.4.2. Manufacturers of the counterfeit / substandard devices do not pay royalties to the owners of essential patents and copy rights.

7.2.5. Environment Impact

7.2.5.1. Contamination from dumping of the e-waste from devices containing forbidden toxic materials; and

7.2.5.2. The dumping site of e-waste material is expensive to maintain and is compounded by shorter lifespan of such devices.

7.3. POSITIVE IMPACTS

7.3.1. Affordability

7.3.1.1. Many users can afford the devices and can get access to services

7.3.2. Tele-Density

7.3.2.1. There is significant increase in mobile telephony penetration due to affordability of these devices;

7.3.3. Economic or commercial

7.3.3.1. the distribution of the mobile devices creates an economic/commercial benefit to those involved in distributing, selling, and repairing such devices.

8. LIMITATIONS IN DETECTING COUNTERFITS

8.1. Counterfeit and substandard mobile devices usually do not conform to any standards whether national, regional or international standards and their International Mobile Equipment Identity (IMEI) numbers usually are neither standardized nor registered with Global System Mobile Communication Association (GSMA). The significant challenges are given below:

8.2. Identification of counterfeit mobile devices

8.2.1. it is not easy to identify counterfeit from genuine devices as they appear physical alike without an additional check layer such as device verification process.

8.3. Type Approval Procedures

8.3.1. The current type approval process is done by reference and analysis of test reports. The absence of a local testing facility means the counterfeits easily come through unnoticed until they are sold to the customer;

8.4. Ports of Entry

8.4.1. There are no rigorous inspections at ports of entry and non-type approved devices easily come into Botswana market.

9. POSSIBLE SOLUTIONS

9.1. This section highlights the processes and technical solutions that could be used to identify and manage counterfeit / substandard devices in Botswana.

9.2. ITU proposes a framework of countering counterfeits. It has passed recommendation or Standards e.g. Technical Solution to Combat Counterfeit, Recommendation Q.5050, model frameworks **(refer to Figure 1 below for the detailed process)**.

9.3. Reference is also made to the international benchmarks which gave insights on the different solutions available to combat counterfeit/Substandard devices in Annexure 3.

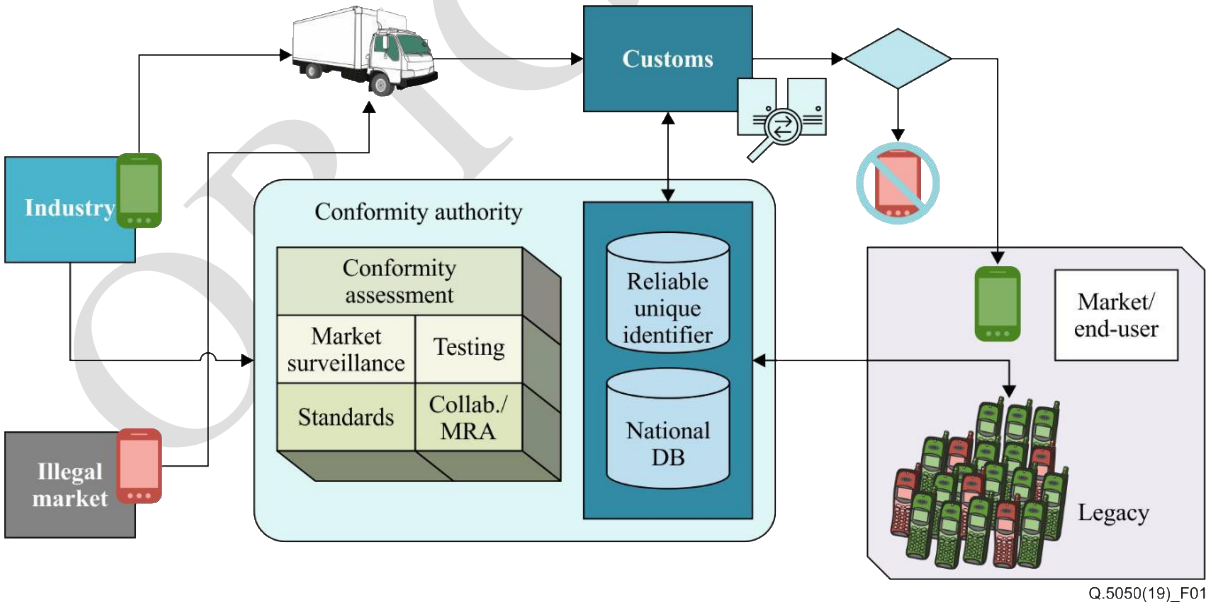

Figure 1: The ITU Proposed General Framework

9.4. The general mobile device framework process for the device quality control:

9.4.1. The public legal instruments (e.g. Trade) allow the checking of the devices entering a country if it is compliant and has a representative/responsible for the devices;

9.4.2. When the devices arrive at the points of entries, an entity (e.g., Customs and the Authority) verify all legal aspects of such devices, including compliance of the devices with any applicable regulatory and certification requirements such as radio frequency allocation, safety and interoperability, etc;

9.4.3. Checks could also be conducted against compliant list to verify that the identifiers of the devices being imported have been legitimately allocated and that the make and model of device being examined matches the details recorded when the identifiers were issued .At this time, non-authorized devices, prevented are from entering the market;

9.4.4. This process is supported by a conformity assessment regime (Type Approval regime) that may be in place;

9.4.5. A database with stored information of the consignment being imported;

9.4.6. Such inventory databases can also support enforcement /inspection activities once equipment (legal or not) is placed in the market.

9.5. Processes (NON-TECHNICAL Systems)

9.5.1. Develop of the guidelines for a specific type i.e. Type Approval (SIM Enabled Devices) Verification Guidelines to augment the Type Approval Guidelines;

9.5.2. Upon adoption of the guidelines, consider process where the existing non-compliant devices would be allowed until end of lifespan;

9.5.3. Establish a collaborative strategic relationship with relevant stakeholders to amplify the overall impact;

9.5.4. Introduce device marking of duly successfully registered devices;

9.5.5. Conduct the mobile device market audit by sampling the devices connected to the networks; and

9.5.6. Raise awareness to highlight the negative implications associated with use of counterfeit.

9.6. Technical Solutions

9.6.1. The IMEI is used uniquely identify mobile devices. It is the only universally applicable and necessary device identifier. The IMEI can be used to identify and deny service to those devices that are not compliant.

9.6.2. They involve implementation of a registration and verification process to uniquely identify devices deserving service. The system involves Analysis Tools for the authentication of the registered devices through the GSMA interface to the IMEI database.

9.6.3. This could be implemented through an open source Type Approval Verification Systems such as DIRBS in **Figure 2** below.

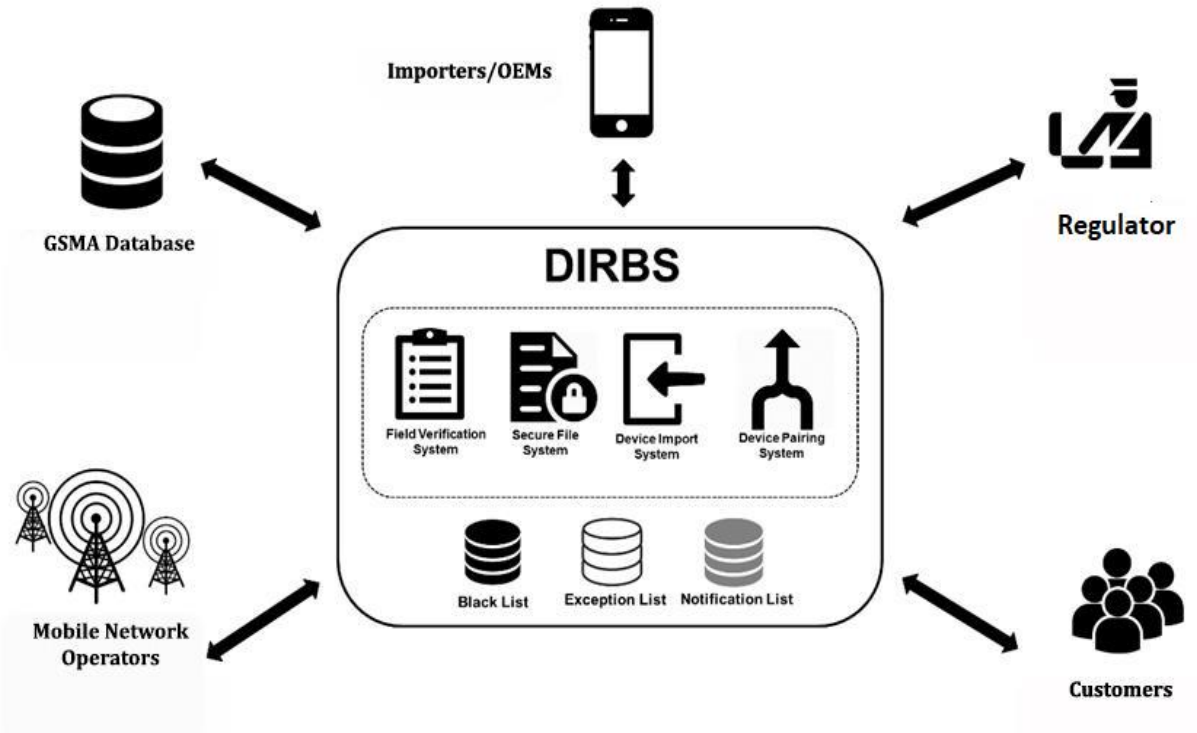

Figure 2: Device Identification, Registration and Blocking System (DIRBS)

9.6.4. The DIRBS platform is the repository for the device identity details in the central identity register (CEIR) collected through the operator's equipment identity register (EIR) mechanisms.

9.6.5. The analysis engine and its associated subsystems provide information to enable device blocking and classification listing (compliant or non-compliant).

10. CONCLUSIONS

10.1. The discussions above have shown the impacts and regulatory challenges of the counterfeits/substandard devices. The use of these devices:

10.1.1. Stifles economic growth and reduces government revenues;

10.1.2. Throttles network capacity and this can be detrimental where the need for bandwidth is envisaged for the new technological advancements;

10.1.3. Exposure to harmful materials and EMF radiation from such devices have adverse effects on consumers and as such pose health and safety risks; and

10.1.4. Exposes consumers to Security and Privacy concerns- these may and may cause privacy violation and identity theft.

10.2. Considering the fast-technological developments, the robust, regulatory frameworks and collaborative strategies are needed to build public support augmented by continuous awareness campaigns and strict market surveillance. The current processes need to be enhanced to deal with this problem.

10.3. To achieve the goals of combatting non-compliant devices, it is important that the Regulator consultation with all stakeholders to adopt ways which will be implementable without stifling the growth of the sector. These objectives will be implemented through the proposed guidelines. There is need to establish a strong collaboration of Private and Public Partnership (PPP), robust

regulatory frameworks, technical solutions, processes and strategies to enhance efforts to counter such activities.