

**COAI Response to TRAI Preliminary Consultation Paper
No. 2/2004 dated 8 January 2004
On
Mobile Phone Theft**

Introduction

1. COAI agrees that there is a need to put in place pre-emptive measures before the problem becomes widespread. We believe that going forward level of security of mobile phones will become increasingly important when the mobile phones will also be used as payment terminals for M-Commerce, which will increase the value of terminals.
2. However, COAI believes that it would perhaps be **desirable if a study were undertaken first, to assess the extent of the problem** that is being caused by stolen handsets before putting in place a suitable mechanism to address the same. It is requested that the **Authority may kindly take the initiative to carry out a study in this regard** and make the results transparently available to all stakeholders.
3. **Various technical methods of securing mobile handsets are being used** in other countries with the objective of safeguarding against misuse of mobile handsets after theft. These include creation of databases to share blacklists of stolen terminals, based on the unique IMEI (International Mobile station Equipment Identity). But to the best of our knowledge, **none of these measures have been successful to any significant extent.**
4. IMEI numbers of many types can easily be reprogrammed. Further, the EU experience has been that very few operators register them in their databases, as they consider it time consuming, customer service unfriendly (call set-up time is delayed by checking the database, the wrong customer may be disconnected) and last but not least costly.
5. From the manufacturers' point of view, each manufacturer uses different methods to make IMEI secure. In the absence of standards, it may both be difficult for manufacturers to declare compliance as well as for public authorities to survey compliance. Further, it **may be very costly to manufacture mobile phones if the identity of the phones could not be changed in both the hardware and software of the phones.** This aspect needs to be especially considered for an acutely price sensitive market like India.
6. We would like to submit that **although various methods may exist to improve the security of the mobile phone, they should be evaluated for ease of implementation, effectiveness as an anti theft measure, cost effectiveness as well as their commercial feasibility for both manufacturers and operators.**
7. To **ensure the effectiveness of any mechanism** introduced by the Authority, it is imperative to ensure that:
 - a. **All stakeholders** – operators, customers, regulatory authorities, law enforcement officials, etc **participate collectively in the process.**

- b. There is a **prescribed uniform way in which the database will be collected and used.**
 - c. **Manufacturers** will have to **work on continuously enhancing and upgrading the security** of the IMEI number whilst at the same time facilitating technological developments/progress under a uniform certification and security system.
 - d. Any **system that is devised by the Authority must be equally applicable to both GSM as well as CDMA handsets.**
8. The **Authority must also look at international precedents and practices** in this regard. Some national EU authorities (UK/France) have introduced national legislation to combat theft of mobile phones. Amongst other things, such legislation provides for the following:
- a. Enabling the police to tackle those fuelling the trade in stolen mobile phones with penalties (UK 'Mobile Telephones Act' up to 5 years prison) for one of the following reasons:
 - Reprogramming the IMEI number
 - Making it illegal to rewrite or change the software of the mobile phone
 - Introducing extra hardware such as new memory or processors to change the
 - Identity

and/or;
 - b. Forces manufacturers to take all technical measures possible to prevent the use of stolen mobile phones (e.g. by complying with –ETSI TS 122.016).
9. However, as no market data exist since these laws have been drafted, their effectiveness in practice is difficult hard to measure.
10. Some of the **issues that must be considered by the Authority** include:
- a. Creation of National databases alone will be ineffective, as stolen handsets may find their way across national borders. **Databases must be linked and all operators must be mandated to register stolen phones.**
 - b. **Developing new technology** as a means to secure the identity of the handset will **entail additional financial investments** for manufacturers and operators. These investments would **lead to higher prices**
 - c. **Manufacturers** should be **required to continuously increase the level of security** in the handsets and they should come up with cost effective standards to do so; Manufacturers and notify bodies should invest in methods to verify and certify security in handsets; Manufacturers should be heard on security issues that could hamper innovation;
 - d. **Co-operation is necessary** between manufacturers, operators and public authorities to **decide on the trade-offs in terms of technology, ease of implementation, cost effectiveness and regulatory.**

11. **Legislation should only be adapted or drafted once the full implication of such legislation is foreseen in terms of:**
- a. Effectiveness of implementation
 - b. Cost to the industry
 - c. Possibility of enforcing the law
 - d. Technology and standardization
 - e. Common standards for measuring
 - f. Effect on future innovation by manufacturers

12. Our issue-wise response to the issues raised by the Authority is given below:

1. **Role of Regulator: The subject of theft of mobile handsets comes under the purview of Law and order which is a state subject in our country. Should TRAI take initiative in mobilizing public opinion, drafting legislation and encouraging the service providers and vendors to take action for minimizing this crime?**

The theft of any property comes under the purview of the Law enforcement agencies. However, since the Mobile phones is the means of connecting to a Cellular service provider and TRAI is responsible for regulation of the telecom market, it is appropriate that **TRAI should take initiative in undertaking public consultations on this issue and make appropriate recommendations** including drafting a legislation which is binding on both the handset manufacturers and the service providers. But, as mentioned earlier, it is first important for the Authority to assess the extent of the problem before putting in place a mechanism to control the same.

2. **Grey Market: In the rapidly growing mobile sector, already more than a million subscribers are estimated to be having handsets from the Grey market. In case, action is taken by the service providers to block the handsets having duplicate IMEI, then a mechanism needs to be evolved and put in place to decide the fate of these subscribers on an individual basis. Suggestions on such a mechanism are requested.**

At first it is submitted that the estimates of the **number of gray market handsets would be significantly higher than the number of 1 million cited by the Authority**. As per estimates by knowledgeable persons, this figure is more likely to be around 14 million, of which a large chunk of handsets may well have duplicate IMEIs. A correct assessment of the number of gray market handsets could well be a defining factor in determining the mechanism to be adopted to tackle the problem of handset theft. The Authority must take a considered view on the matter after giving due weight to the fact that a large chunk of the existing subscriber base, especially the **low end and marginal subscribers, could well have gray market handsets with duplicate IMEIs and would be adversely affected by any stringent action taken by the Authority**

Further, while the incentive for consumers to seek out the gray market will be lower because of the reduction in duties, however, it is quite likely that the **gray market would continue perhaps as a second hand handset market with first time**

consumers / users preferring to buy an affordable second hand handset rather than a brand new handset. The issue would then arise as to how second hand handsets can be distinguished from stolen handsets so as to protect the consumers. A strict action on stolen handsets could also nip the flourishing second-hand handset market that is providing a low entry opportunity to first time / low end users. Thus the Authority must weigh the pros and cons of putting in place a **stringent law / procedure on stolen handsets that may have an entirely adverse effect on a legitimate second hand market.**

It is submitted that the **Authority will first have to be put in place a suitable legislation and only once that is done that suitable actions can be taken towards enforcement.**

Legislation if any would be prospective in nature. It would not take care of, at least in the short to medium term, the problem of a large number of Handsets that exist currently with duplicate IMEIs, and thus do not comply with the new regulations imposed on the handset manufacturers. There will thus be **an interim period when the mechanism is not entirely foolproof and may in fact impact the customers,** holding a genuine handset as well as ones having a gray market handset. The problem at hand is that a large number of handsets exist with duplicate IMEI numbers which if blocked may lead to a genuine customer being affected.

- 3. Procedures required for collection/update of data and interaction amongst the relevant entities: It is necessary to devise procedures for collection and use of data as well as the interaction of operators, consumers and other stakeholders in this exercise. These procedures should be easy to implement and not impose great costs on the persons/institutions involved.**

For the purposes of data exchange between relevant entities, **the manner in which the European operators use their CEIR should be the manner for the use by the Indian operators as well.** Also, the proposed CEIR should be linked to the European CEIR.

- 4. Ownership and cost implication of setting up of CEIR : For implementing the given scheme, a number of steps namely preparation of database of all the available IMEI's, regular update of database in the EIR, creation of CEIR and its regular update will be involved. This will involve participation by all the service providers operating in the country. Moreover, a Central Equipment Identified Register (CEIR) will need to be created and regularly updated. All this will involve certain cost and constant monitoring. It needs to be deliberated and decided whether this control should be done by an agency like OMBUDSMAN or by some association like COAI, or by the Regulator i.e., TRAI.**

The European operators have joined hands with the help of GSM Europe and are maintaining a Central Equipment Identity Register (CEIR). However, it is very important to note that **in the European markets, more often than not, the service provider bundles the handset along with the service.** This is not the case in India where it is the customer who generally buys the handset and the service p[rovider has absolutely no control in the matter. So it is easier for the service

providers in Europe to ensure that unauthorized handsets are not used on their network. **This aspect must be kept in mind by the Authority whilst finalizing its recommendations.**

As regards the administration and control of the CEIR, it is suggested that the **regulator as an independent organization must maintain this database.** This database must be updated on a daily basis to ensure its relevance and effectiveness. This database must be also shared with all service providers who would be required to check the centralized blacklist before activating a new subscriber.

It is once again **reiterated that the mechanism adopted by the Authority must be equally applicable to CDMA handsets as CDMA subscribers now constitute around 20% of the market.**

5. **Legislation: Apart from blocking all the handsets, a legislation making reprogramming of IMEI as an offence is also required so that the recycling of handsets after changing the IMEI is deterred. Countries like France, Germany, Greece, Spain are already considering making it an offence. In India also a legislation on the same lines may be required to be enacted in order to make reprogramming of handset for the purpose of changing the IMEI as an offence. Please comment.**

Legislation making reprogramming of a handset an offence is an absolute prerequisite. The important point to note here is also that **an even more stringent legislation needs to be brought on the vendors supplying the handsets.**

The **Authority may examine the processes and procedures being adopted by GSMA and the EICTA** who are in the process of drafting the mandatory requirements for the handset manufacturers, which is scheduled to be presented in the 3GSM Association meeting in the first quarter of 2004.

COAI believes that the **India should follow the same legislation** so as to ensure that the compliance norms are the same and India does not become a secondary market for the Handset manufacturers or handsets that cannot be used in Europe.