VODAFONE ESSAR's RESPONSE
Issues relating to blocking of IMEI for lost /stolen mobile handsets

INTRODUCTION

IMEI (International Mobile Equipment Identity), uniquely identifies a specific mobile phone on a mobile network and though the potential to use this number to identify stolen handsets and prevent them from accessing a network to place calls exists, implementing this involves significant cost which would throw up some unique and serious issues like:

- creation of the infrastructure;
- the cost of this infrastructure
- whether the benefits are commensurate with the costs

The percentage of handsets reported as stolen is not a significant number that would justify the creation and maintenance of an infrastructure of this nature. Especially on account of the fact that implementing the Central Equipment Identity Register (CEIR) by itself is highly unlikely to contribute to the reduction of thefts or misuse of such handsets.

The issue which requires greater attention and some kind of a solution is to discourage reprogramming of handsets or replication of IMEI numbers on handsets. For example when handsets with the same IMEI are floating around in the market and if various operators have these activated in their network, what happens when one of these handsets is reported to be stolen?

Will all of the handsets with similar IMEI across all networks be blocked? Which of these handsets is genuine and which one is not? Would blocking be a practical solution?

We are flagging this issue at the very outset to highlight the gravity of the bigger problem – and the need therefore to implement a solution that addresses multiple aspects of the problem – without which the main objective may not be achieved.

We are pleased to submit below our observations on the issues raised by the Authority for consultation.

OBSERVATIONS ON SOME OF THE GENERAL ISSUES RAISED IN THE PAPER

Today, in case of theft of a mobile phone, on complaint the service providers are providing the facility of blocking the SIM card. In order to block SIM card, the subscriber need to report the theft to the service provider's call centre.

VF
The SIM card is the repository of a customer's identity, choice of services, the customer's MSISDN and often the customer's contact list and directory. A SIM card is issued by the service provider to provision and activate services on a customer's handset and is non-transferable. The SIM card also contains information that is used for billing the customer.

The possibility of a customer's identity and account being misused on account of a stolen SIM is much higher and thus the urgency to block all services attached to a SIM is vital.

RESPONSE TO QUERIES

1. In order to reduce/discourage mobile theft do you think the blocking of IMEI is an effective solution? Please give reasons

   VF

   The incidence of handset thefts in the telecom sector as a percentage of the total subscriber numbers or handset sales is not really large. Further thefts of handsets are more of a law and order issue than an operator/service provider issue because customers purchase handsets directly. There are millions of locations and outlets from which a customer can chose to purchase a handset and there is no practical method to monitor or control this.

   This is unlike many markets where handsets are almost nearly always bundled with a set of services. Operators probably absorb the cost of a handset in return for a customer staying with the network for a minimum period of time and use the services. Thefts of such handsets often mean use of services along with the handset and thus blocking of the handset is important – much like blocking of SIMs provided by operators here.

   Further, as highlighted in our introduction, there is no fool proof mechanism today to ensure only unique IMEI handsets are in use and if one handset is reported as stolen, there is no guarantee that many other genuine users in the country are not using handsets with the same IMEI. Blocking of the handset in such a scenario is thus unlikely to prove to be a solution.

   Thus any decision to enforce a CEIR should be carefully considered and supported by supporting legislations to make the solution effective. Primarily:

   - Restrictions on the reprogramming of devices should be enforced;
   - Ensuring no misuse of the blocking facility by requiring proper authentication of ownership of handset that is being reported as stolen
   - Ensuring responsibility on the owner of the handset since this is a law and order issue
   - Most importantly ensuring that similarly numbered IMEIs are not active in other networks at the same time.

2. In case blocking of IMEI is implemented, to what extent load on the network will increase? Please give details

   VF

   If the CEIR is implemented there is a very real possibility of degradation of the QOS levels on account of the following:

   - Today the handset IMEI is validated from a white list whenever a call is initiated.
   - The white list is synchronized with the GSMA database of IMEI numbers.
   - For every event (a call, SMS, MMS etc) initiated by a user the MSC checks the IMEI from this white list the call is allowed if the entry is found in this list. If not, the call is not permitted.
   - Now, in the proposed regime, there will have to be a new list of "stolen" handsets (a black list) to be managed.
   - Thus, there will be need to first dip in into the "blacklist database" (which will keep growing over time as the provision for deleting of stolen handsets may not be practical; thus this black list could assume large proportions over time);

- Thereafter, the call will check the "white list" database.
- These actions will definitely load the networks significantly leading to a decrease in capacity and increased call connect times.

We thus request the Authority to consider all these aspects in detail as QOS would be affected for all subscribers.

Further, similar querying is an integral feature for MNP; and now there is the new requirement to filter telemarketing calls. These are all incremental increase in call processing and completion time frames. Customer experience would suffer on account of this.

3. In your opinion who should maintain the CEIR? Please give reasons

VF

As submitted above, we are not sure about the utility of the CEIR without supporting legislations and regulations.

Apart from the capital expenditure for such a facility there will be regular upgrades and operational costs which would make it an expensive proposition to maintain. It would best be maintained by a central government organization like the NIC – which is running the national do not call registry today.

4. Should the CEIR be maintained at national level or zonal level? Provide details including the estimated data size

VF

The CEIR should be a single national level database.
Multiple databases would create huge problems of interconnection, disaster recovery, updation and synchronization etc.

5. Please comment on cost and funding aspects of Centralized EIR? Please provide detailed cost estimates?

VF

The cost components of such a CEIR would involve servers, various kinds of hardware and software, processing and storage capacity, cost of connectivity, administrative costs of data center and hosting, regular maintenance, upgrades and security etc. Providing a detailed cost break down would involve a detailed costing exercise.

6. Should blocking of IMEI /ESN be chargeable from customer? If yes, what should be the charge?

VF

If such a blocking service is implemented, customers should have to pay for availing this service.

7. Please give your views on bringing a legislation to prevent reprogramming of mobile devices? In your opinion what are the aspects that need to be covered under such legislation?

   VF

   As already highlighted by us earlier, the CEIR alone is not likely to provide a viable solution. There is need to evolve some stringent rules and legislations to prevent reprogramming and reuse etc.

8. What should be the procedure for blocking the IMEI?

   VF

   The process for accepting customer requests for blocking of handsets should follow a very well laid out process:

   - Customer who loses the handset files an FIR with proof of handset ownership
   - The FIR is quoted along with IMEI number and the request for blocking the handset to the operator is sent with a copy of the FIR
   - Operator verifies the SIM details and the corresponding IMEI details in the database before initiating the block

9. If lost mobile is found, should there be a facility of unblocking the IMEI number? If yes, what should be the process for it? Should there be a time limit for unblocking the IMEI number? Should it be chargeable?

   VF

   Unblocking of mobiles may be a difficult and cumbersome exercise and definitely not possible if requested after more than 30 days. Retrieval of data for such an action beyond this period would not be reasonable.