mobile device counterfeit detection and eradication

TToday's global economy depends upon the integrity and security of a mobile ecosystem to the benefit of all stakeholders. That's why the continuing prevalence of counterfeit phones around the world needs to be addressed by the industry.

According to the Mobile Manufacturer's Forum (MMF), there are 148 million counterfeit mobile phones worldwide resulting in $6 billion in revenue losses to the mobile industry and governments globally. In India alone, the MMF estimates that counterfeits make up more than 20 percent of the mobile phone market, costing the industry $1.5 billion annually in lost sales and the government $85 million in direct tax losses and roughly $460 million in indirect tax losses.

But counterfeit devices not only hurt original equipment manufacturer (OEM) profits and government tax revenues -- they adversely impact the entire mobile ecosystem.

Consider the user who often doesn't realize they are purchasing a counterfeit phone. Counterfeit phones have been shown to contain dangerous levels of chemicals and metals such as lead up to 40 times higher than industry standards. The devices generally run on inferior operating systems and often include applications that illegally collect personal data. Also, many consumers inevitably experience malfunctions with their product and falsely assume it's under warranty by a genuine manufacturer.

Since the devices are generally not tested under telecommunications compliance standards, counterfeit phones also experience frequent call drops. This adversely affects the user and the service provider by degrading coverage, call quality and mobile internet speeds on the network. MMF research found that as network coverage decreases due to substandard connected devices, coverage black spots can only be fixed by installing more base stations, a significant financial outlay for service providers. Service providers also suffer reputation damage due to the perceived low network quality by subscribers.

There are impediments to aggressive action from some stakeholders in the mobile ecosystem to stopping counterfeit devices. Service providers, for example, fear losing subscribers and average revenue per user (ARPU) if counterfeits are removed from the market. In many developing countries, government regulators are wary of blocking service for counterfeit devices that are popular among those in the lower socioeconomic levels of society, making it a combustible political issue. But these are short-sighted responses, ignoring the significant, long-term negative impacts of counterfeit mobile devices.

Limitations of Current Solutions

There are several solutions currently in place by individual countries for detecting and removing stolen phones – but not counterfeits -- that leverage the International Mobile Equipment Identity (IMEI) database by the GSMA.

The IMEI is a unique identifier for every mobile phone that is manufactured. Service providers can identify IMEIs associated with lost or stolen devices reported by subscribers. GSMA then aggregates the information and disseminates the list of blacklisted IMEIs to the Equipment Identity Register (EIR) for each carrier so other service providers can block the devices from being used on their

http://spotafakephone.com//docs/eng/PR_MMF-Counterfeit-mobile-phones-USD-6-billion-drain-on-global-economy_EN.pdf trademark, and iconectiv is a trademark, of Telcordia Technologies, Inc. dba iconectiv ("iconectiv").

There are impediments to aggressive action from some stakeholders in the mobile ecosystem to stopping counterfeit devices. Service providers, for example, fear losing subscribers and average revenue per user (ARPU) if counterfeits are removed from the market. In many developing countries, government regulators are wary of blocking service for counterfeit devices that are popular among those in the lower socioeconomic levels of society, making it a combustible political issue. But these are short-sighted responses, ignoring the significant, long-term negative impacts of counterfeit mobile devices.

Limitations of Current Solutions

There are several solutions currently in place by individual countries for detecting and removing stolen phones – but not counterfeits -- that leverage the International Mobile Equipment Identity (IMEI) database by the GSMA.

The IMEI is a unique identifier for every mobile phone that is manufactured. Service providers can identify IMEIs associated with lost or stolen devices reported by subscribers. GSMA then aggregates the information and disseminates the list of blacklisted IMEIs to the Equipment Identity Register (EIR) for each carrier so other service providers can block the devices from being used on their networks.

In India, mobile devices coming through customs require a government-mandated IMEI certificate. The mandate came about due to a high court case brought by OEMs who were seeing revenue leakage and market dilution due to counterfeits. In Sri Lanka, regulators post a Type Approved Devices list on their websites that provide the approved range of IMEIs allowed in their country. In Oman, subscribers can access an SMS-based service to verify the IMEI of their mobile device.

Unfortunately, these solutions are not enough. Counterfeit devices often feature legitimate IMEI numbers that match one or more of the IMEIs already in use or approved for use in the country.

Without knowing if an IMEI identifier has counterfeit clones, a legitimate phone can be blocked for service in addition to thousands of counterfeit clones with that identifier on the network. Some service providers who have blocked an IMEI device have reinstated it due to the huge loss of ARPU.

are imported but have not resulted in any taxes or custom duties. Any devices not on the list of legal devices would be blocked from import. Devices that are not imported would be flagged as well, but in most countries mobile devices are imported and sold through service providers and marketplaces.

Consumers looking to buy a device could confirm that the device is authentic by accessing a public portal of the device registry. If a device they already own is proven to be counterfeit, lost, stolen or on any other blacklist, they can report it to the registry which will result in blacklisting the IMEI on networks.

distributors to ensure resolution of any outstanding issues.

The Device Registry Solution

A single device registry for all mobile phones would serve as a better, more comprehensive global solution for the detection of counterfeit devices and removing them from service provider networks. The goal of the centralized platform would be to create significant benefit for all stakeholders that would encourage their participation and support.

How would a global device registry system work in each country?

First, service providers would start by inputting the "triplet" of mobile device identifications – IMEI, IMSI and MSISDN – into the platform. Optimally, other information such as the owner, device, carrier and purchase time, date and location would be included as well. In addition, carriers would submit the blacklisted devices on their network, whether lost, stolen, counterfeit, etc. This list would be distributed to all other carriers in the country to halt the spread of counterfeit devices by making it more difficult for those who purchase them to gain network access. The information would also be aggregated and used to detect clones from duplicate identifications in the inputted device data.

Customs departments could take another tack and create a "white list" by inputting the IMEIs from a list of legally imported devices from OEMs, suppliers and distributors. These would be used to determine if there are devices in the national network that are imported but have not resulted in any taxes or custom duties. Any devices not on the list of legal devices would be blocked from import. Devices that are not imported would be flagged as well, but in most countries mobile devices are imported and sold through service providers and marketplaces.

Consumers looking to buy a device could confirm that the device is authentic by accessing a public portal of the device registry. If a device they already own is proven to be counterfeit, lost, stolen or on any other blacklist, they can report it to the registry which will result in blacklisting the IMEI on networks.

distributors to ensure resolution of any outstanding issues.

In case there is a discrepancy regarding a particular number range, iconectiv will investigate the matter directly with the number administrator of that country without any extra charge.

iconectiv offers flexible delivery options for : TruNumber Routing* data including:

- Secure File Transfer Protocol (SFTP) downloads
- ENUM query service
- SOAP/XML for near real-time incremental downloads

routing at a glance

- Stop fraudulent calls to high-risk number ranges
- Obtain early warnings on impending fraud attacks
- Prevent revenue leakage, routing errors and interconnection charges with optimal, least-cost routing

As the system continuously analyzes which devices are illegal from the various inputs, results could be published or easily researched by incorporating business intelligence and data analytics. All stakeholders, from regulators and customs to service providers and subscribers, could be given some level of appropriate access.

Once the reports on counterfeit devices are in, service providers can notify relevant subscribers and, depending on the policies they have in place, begin the process of resolution and eradication of the devices from the network. Regulatory agencies and service providers in each market will decide the measures taken towards counterfeit eradication and whether the consumer pays for the new device or if it is provided as part of a contract or some other fair remedy.

Regulators can also verify service provider compliance and leverage trends gleaned from device-based analytics to ensure their policies are working as planned.

Customs departments can work in tandem with law enforcement and government agencies to crack down on fraud and stop the growth of counterfeit devices and loss of tax revenue. Customs can also reach out to the relevant OEMs, suppliers and distributors to ensure resolution of any outstanding issues.

Clear Benefits

The existing mechanisms to curtailing counterfeit mobile devices are simply stop-gap measures that can be circumvented and do not provide a common platform to tackle the issue through mobile device-based identity.

The benefits to the mobile ecosystem stakeholders are clear:

•OEMs and customs will benefit the most in terms of monetary value since the system will eradicate counterfeits and fraud through averting custom duties/taxes;

•Regulators will also benefit by removing counterfeits that are a public hazard and harmful to the mobile economy. Also, the device registry could be expanded to new types of devices coming to market, such as IoT devices;

•While service providers may initially view this as loss of ARPU, removing counterfeit devices will enhance the customer experience, reduce the need for base station construction, and ensure device integrity for deploying value-added services such as mobile payments;

•Law enforcement agencies could more easily track illegal phones being used on a network, assisting them in their pursuit of those using illegal devices in the commission of a crime;

•Subscribers will have a convenient and reliable one-stop shop to validate a device before purchasing and obtain assistance as needed.

Utilizing a device registry platform approach will support economic growth by tackling counterfeits, ensure mobile device integrity and serve as a foundation for IoT-related device management in the future.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800

info@iconectiv.com

www.iconectiv.com

iCOL-MB-ID-E-LT-001, Apr2019