

April, 2018

Using IMEI control systems to combat stolen,
fraudulent, and counterfeit
mobile phones: **A Colombia case study**

By Jay Gumbiner

IDC Latin America

IDC# LA18004



Executive Summary

What is the problem?

As the ubiquity of the mobile phone in society has exploded over the past decade, it has become a target for criminal organizations and illegitimate manufacturers. Based on research conducted by the International Telecommunication Union and the European Union Intellectual Property Office in 2017, illegal mobile phones across the world contributed to 12.9% of lost sales for legitimate manufacturers/distributors in 2015¹. Criminal organizations in Latin America and across the world are stealing mobile phones at greater rates as a source of income or as a means to allow them to operate under the radar of law enforcement. Illegitimate manufacturers are shipping increasing volumes of counterfeit and fraudulent mobile phones that contain stolen intellectual property and malware, and are often not designed to meet the established regulatory requirements or quality levels. The risks to consumers cannot continue to be ignored; whether knowingly or unknowingly purchasing a poor-quality counterfeit phone or being caught up in a violent crime from an attempted phone theft, ever more consumers are being put at risk.

Beyond the obvious issues related to personal safety and associated crime committed with stolen or fraudulent phones, as well as the revenues that are lost by legitimate manufacturers, these devices also often cost governments millions a year in less import and/or sales tax revenues in addition to a significant number of direct and indirect lost jobs.

Due to poor design and low-quality components, fraudulent and counterfeit phones also lead to degraded user experience, not just for those users with such devices, but for all users on the network due to an overall reduction in network capacity resulting in increased capital and operating expenditure costs for the network carriers.

¹ The Economic Cost of IPR Infringement in the Smartphones Sector, Authors: Nathan Wajzman, Carolina Arias Burgos; February 2017; European Union Intellectual Property Office

Globally, non-compliant or illicitly obtained phones are increasingly connecting to mobile networks with negative consequences for consumers, operators, manufacturers and governments. What can be done to mitigate this growing problem?

How is Colombia solving this problem?

Initially designed to help combat the growth of stolen phones within the country, in 2011 Colombia's government, in collaboration with different sectors such as defense, ICT, retail, and customs, among others, through the national telecommunications regulator CRC (Comisión de Regulación de Comunicaciones -Communications Regulatory Commission-) and MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones -Ministry of Information Technology and Communications-) developed and implemented a technology-based system to enable identification, registration, and network access management of devices connecting to the nation's cellular networks.

This IMEI²-monitoring system allows the continuous monitoring of mobile phones as they connect to the nation's networks, ensuring that only legal and legitimate devices can be used. Irregular devices are either immediately blocked from the system in the case of a reported stolen/lost phone, or in some cases the user is informed of the potential blocking of the phone with invalid identifying information and the eventual blocking of the phone if certain procedures to 'validate' the phone are not completed.

What are the benefits of an IMEI-control system?

An IMEI²-control system like what was deployed by the CRC in Colombia has numerous benefits driving value for nearly everyone in the ecosystem:

- **Government:** grows legal taxation, improves security and helps fight against the theft of mobile devices.
- **Regulator:** improved management of the devices connecting to mobile networks, including public safety certifications, more efficient use of a scarce public resource, radio spectrum, and maintains the integrity of the mobile device identifiers.

² The International Mobile Equipment Identity (IMEI) is based on a technology standard (ETSI 3GPP TS 122 016 v13.0.0 (2016-02)) which requires each device to have a globally unique IMEI. The IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device.

- **Operators:** Improves the customer's perception of security and protection. Counterfeit and fraudulent devices have proven to have significant performance degradation relative to legitimate devices resulting in reduced network capacity and increased costs.
- **Legitimate Manufacturers:** increased sales from eliminating illegal and unfair competition.
- **Consumers:** Reduced threat of crime as stolen phones have less value and protection against low-quality knock-offs (which may have malware, excess radiation, false device specifications and poor voice/data connections).

By focusing on a handset IMEI-control approach, the solution in Colombia attempts to solve the issue of stolen and fraudulent phones at its root. If an irregular phone cannot be connected, or continue to be used, there is less incentive to either steal a phone or purchase a counterfeit or fraudulent handset. The industry needs these solutions more widely deployed in countries across the world to ensure one country's illegal devices do not simply relocate to another country lacking a proper solution. Every country is at risk and the problem needs to be addressed globally.



An **IMEI**-control system like what was deployed by the CRC in Colombia has numerous benefits driving value for nearly everyone in the ecosystem

What should the regulators be doing now?

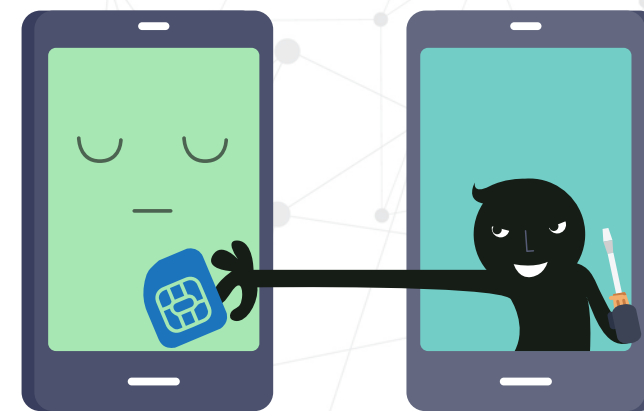
The regulators do not need to reinvent the wheel when it comes to creating solutions for their respective geographies. The first step should be engaging with experienced subject matter experts to get help assessing and quantifying the issue while learning about the solutions available to meet their country's specific needs. Ensuring that the solution is not only scalable and adaptable, but can be implemented with the right business rules to continuously monitor, notify, and manage the user base is paramount. Awareness campaigns targeting retailers, distributors, traders, importers, and customers are important to ensuring the ecosystem is prepared and ideally prevent the devices from being purchased or imported in the first place. It is also important to engage other regional entities or neighboring regulators to optimize the solution for each country.

This document describes major findings in research conducted by IDC on the implementation of the phone identification, registration, and blocking system that CRC has put into place in Colombia and can be used as a potential blueprint for other governments, regulators, or mobile operators considering solutions for their respective geographies to help minimize fraudulent, counterfeit, or stolen phones from connecting to the networks, ultimately leading to higher quality phone connections for its citizens, higher tax revenues from legitimate phone sales within the formal economy, and lower associated crime rates currently associated with stolen phones.

FRAUDULENT & ILLEGAL MOBILE DEVICES: AN ECOSYSTEM PROBLEM

In Latin America in 2018, 173 million mobile phones are expected to be sold in the region, of which nine out of ten devices will be smartphones. To put this into perspective, the figure is 16 times the size of the smartphone market merely 10 years ago. With the explosion of mobile phone penetration in Latin America over the past decade, the ability for consumers, telco operators, retailers, manufacturers, governments, law enforcement, and regulators to stay on top of the latest trends has become more challenging.

As the subsidy-based pricing model for phones has been decreasing over the past few years and the resulting 'open-market'³ has seen strong growth in Latin America, the potential connections of counterfeit or fraudulent devices also increased substantially. These fraudulent handsets cause a myriad of problems for consumers, governments, telco operators, and manufacturers, among others, but industry players have been working together to create solutions to help identify and stop these harmful phones from connecting to the networks. One successful solution could be the one that has been implemented in Colombia to fight the theft of mobile devices and IMEI tampering to circumvent the blocking of reported stolen IMEIs, which will be explained in further detail, as an effective IMEI-blocking system. Before reviewing the details and experience of Colombia, it's important to first identify the different types of fraudulent devices.



3. Open market phones refer to handsets not sold directly by a telecom operator and sold with no carrier-initiated subsidies; 47% of all smartphones sold in 2016 in Latin America were through the open-market

WHAT ARE EXAMPLES OF FRAUDULENT AND ILLEGAL DEVICES?

Fraudulent mobile devices are devices that fail to comply with various international standards, specifications, and guidelines, including IMEI usage, certification/type approval requirements, customs and local tax regulations, or adherence to intellectual property (IP) rights. Fraudulent device types are further defined in Table 1:





TABLE 1

Common Examples of Fraudulent, Non-compliant or Illegal Devices

Types of Fraudulent, Non-compliant and Illegal Devices	What is it?
Invalid or malformed	Lacks an official standardized IMEI format/code
Duplicated IMEI	Has a non-unique number or is programmed in two or more devices
Non-Homologated or Type Approved phone	Phone has not been certified by regulatory authority to allow connection to the country's mobile network
Stolen	A phone that has been reported as stolen
Counterfeit	A phone that infringes another company's intellectual property (trademark, copyright, patent)

WHO IS IMPACTED BY FRAUDULENT, NON-COMPLIANT AND ILLEGAL DEVICES AND HOW?

TABLE 2

Impacted	What's the Impact?
 Consumers	Dropped calls, slower handoffs, slower data speeds, health and safety risks (dangerous levels of certain materials and radiation energy)
 Governments	Lower tax revenue, increased opportunity for crime, public safety risk
 Operators	Reduced network capacity, increased capital and operating expenses
 Manufacturers	Lower sales, less resources to spend in R&D



II. HOW COLOMBIA ADDRESSED THE THEFT OF MOBILE DEVICES WHICH ALSO HELPED TO CONTROL FRAUDULENT AND ILLEGAL DEVICES

In order to control the theft of mobile devices and the tampering of stolen handsets which are reintroduced into the market, as well as ensuring that all the phones connecting to the nation's mobile networks were legitimate phones that had been homologated and legally imported into the country, the government began to put a strategy in place seven years ago to begin establishing a framework for identifying the phones entering the country or connecting to the networks and a plan and process for blocking those identified as irregular⁴ or stolen.

In 2011 Colombia's telecommunications regulatory authority CRC, together with the cooperation of the ITC Ministry and the country's telecom mobile operators, set out to focus on three main areas to help address the risks associated with stolen and tampered phones:

- Reducing the drivers in the market that facilitate the illegal business of handset theft.
- Combating the illicit economy supporting this ecosystem.
- Educating the public about the risks associated with such devices and the need for purchasing legal phones in authorized points of sale.

The decision was made to address the problem by deploying a centralized database made up of a positive and negative registration list, under the legal and financial responsibility of the mobile operators through a private third party. The positive database repository (works off-line in respect to the mobile network) identifies and registers all legally imported and acquired IMEIs that are approved for use in the country, while the negative database establishes and maintains a blacklist of IMEIs that should not have access to the networks (blocked).

It is critical at the early stages of such an initiative to establish the necessary legal basis for managing access to the nation's mobile network, and so in 2011 the CRC passed a series of resolutions to help facilitate this process. These included a host of resolutions that addressed many issues such as facilitating the sharing of data between different entities, defining the technical aspects and rules for creating,

4. Within this category the Colombian government includes devices that have been stolen that are tampered with in order to be reintroduced into the market showing up in mobile networks as unformatted, invalid, non-homologated or not registered IMEIs



updating, and managing the databases that are used to block phones that have been reported as being stolen, defining phones without a valid TAC⁵ assigned by the GSMA⁶ as an 'invalid IMEI', as well as making it the user's responsibility to ensure their device is properly homologated or approved for use in the country, and registered in the positive database, since it's a requirement in Colombia.

The first step was the creation of two databases, known as the 'positive' and 'negative' lists, which is analogous to a whitelist and blacklist of IMEI numbers. The positive list includes all those IMEIs associated with phones that have been legally imported and acquired, that are homologated and approved for connecting to the local networks and are associated with the required forms of identification for the Colombian consumers. The blacklist would include those phones that:

- Are reported as lost/stolen
- Have an invalid IMEI (neither in GSMA nor CRC TAC list)
- Are not homologated
- Have been detected as duplicated (cloned in another device different from the genuine one)
- Have not been registered in the positive database.

The malformed IMEIs (extra digits, lack of digits or containing letters) have not been able to connect to the networks since February 2017.

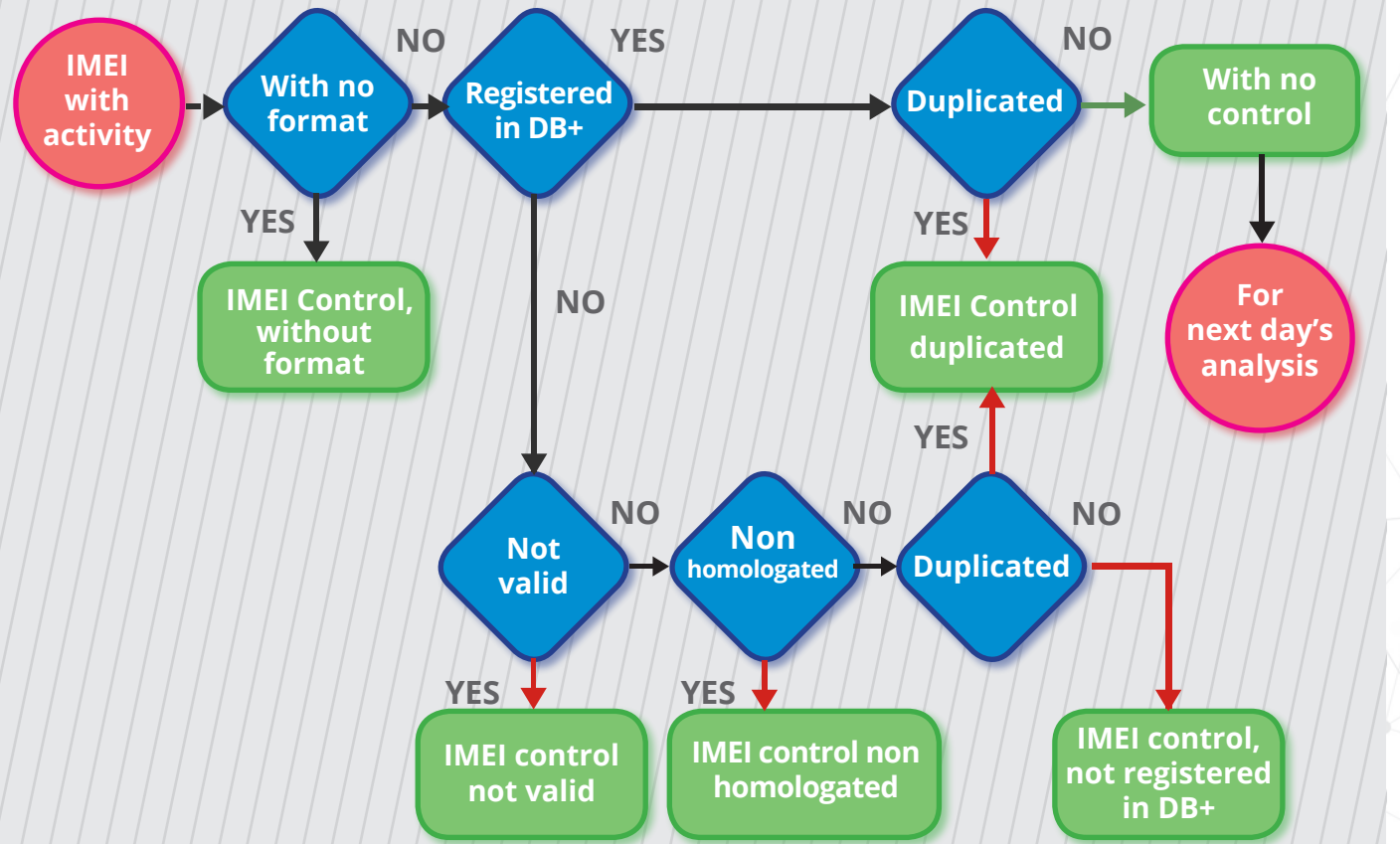
As seen in Figure 1, one can follow the instances in which the phones could be flagged for potential blocking, which includes IMEIs with incorrect number formats, invalid IMEIs, non-homologated phones, cloned IMEIs, or not appearing in the positive database. An additional scenario is for those phones which have been reported as stolen or lost by the owner.

5. Type Allocation Code. This is the first eight-digit portion of the IMEI's 15 digits. It identifies the specific device model.

6. GSM Association. An association that groups mobile carriers and operators to regulate, implement and promote the GSM mobile telephony. GSM stands for Global System for Mobile Communications.

FIGURE 1

Priority Flow of Control Measures



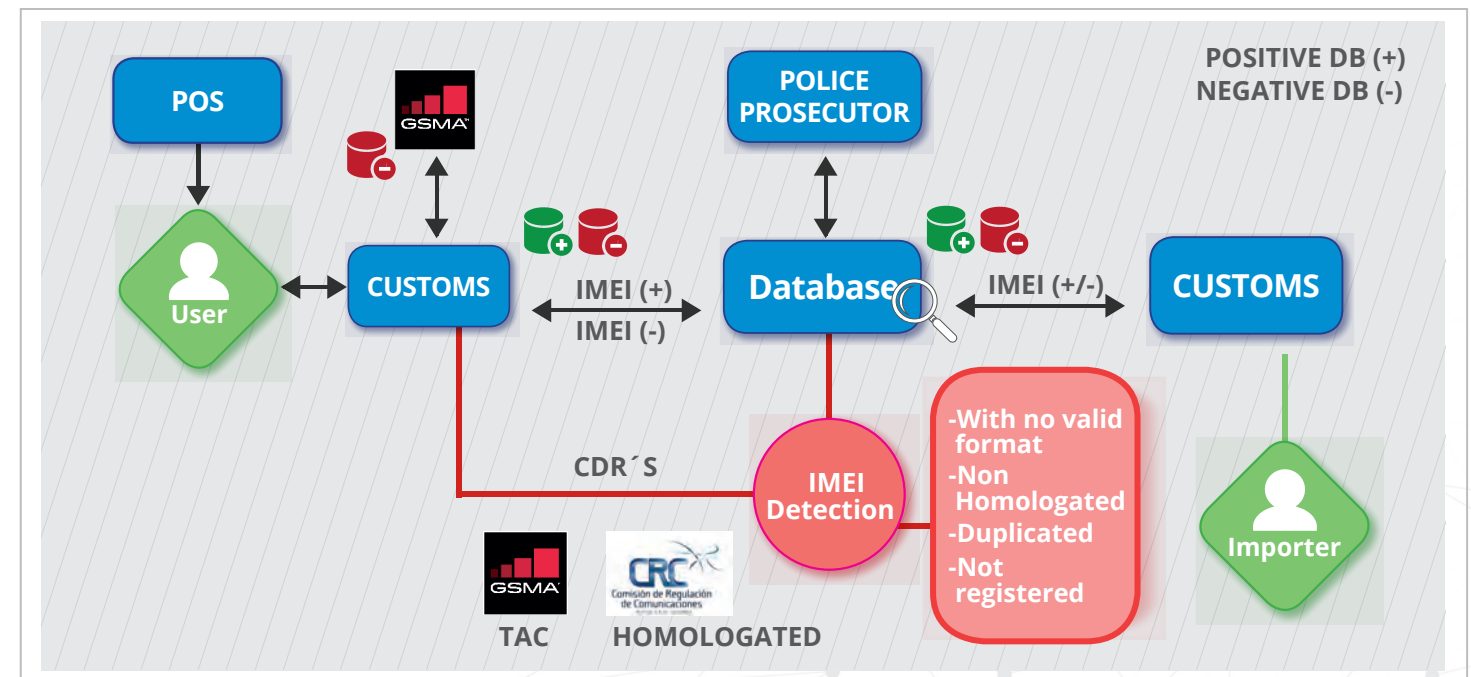
Source: CRC, 2016; Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: Etapa de control, Relaciones de Gobierno y Asesoría.

In 2011, Colombia's Law 1453 Article 106, authorized the centralized databases which were implemented by the Spanish firm, Informática El Corte Inglés S.A. The cost was absorbed by the Colombian mobile operators and divided up per an agreed-upon plan negotiated between the operators themselves. The mobile carriers in Colombia also have employees working in internal 'fraud' departments that manage the IMEI database and blocking process, as well as other issues related to fraud which can go beyond just the stolen and tampered with phones and includes issues related to phone lines and bills. IDC estimates a total 30 employees spread out across the 9 physical and virtual mobile phone carriers in Colombia having a fraud prevention role.

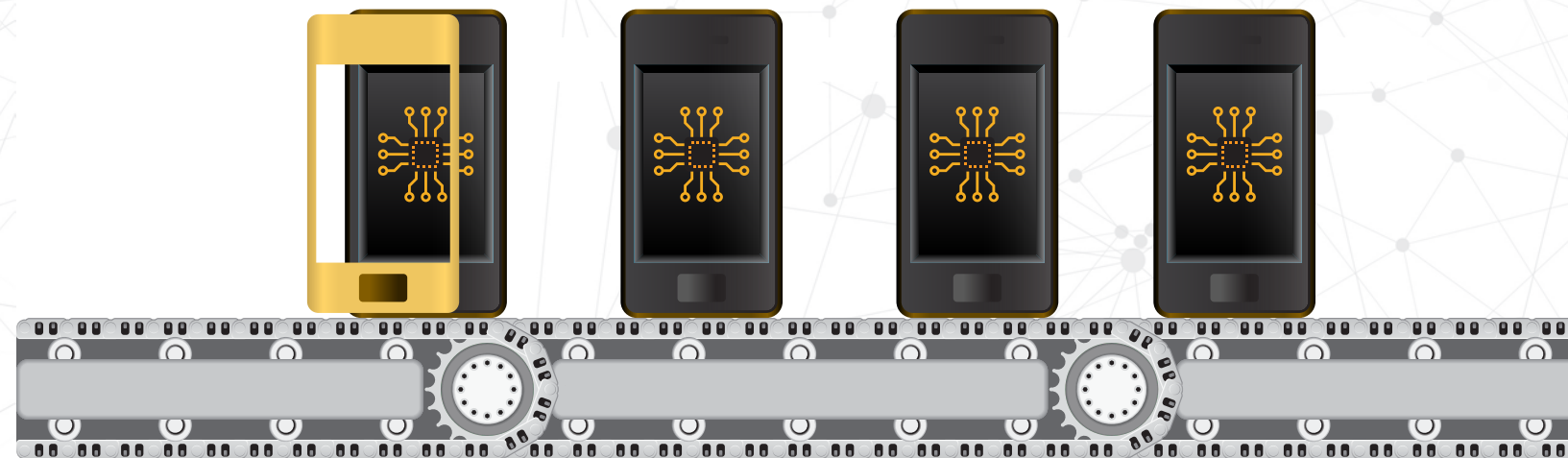
Colombia decided to phase-in the blocking schedule over time to minimize the impact to users and ensure implementation went smoothly by first targeting stolen devices and those not registered in the positive database, then the ones with invalid IMEIs before moving on to the other categories of irregular devices.

Figure 2 shows the system of IMEI control deployed in Colombia after five years.

FIGURE 2

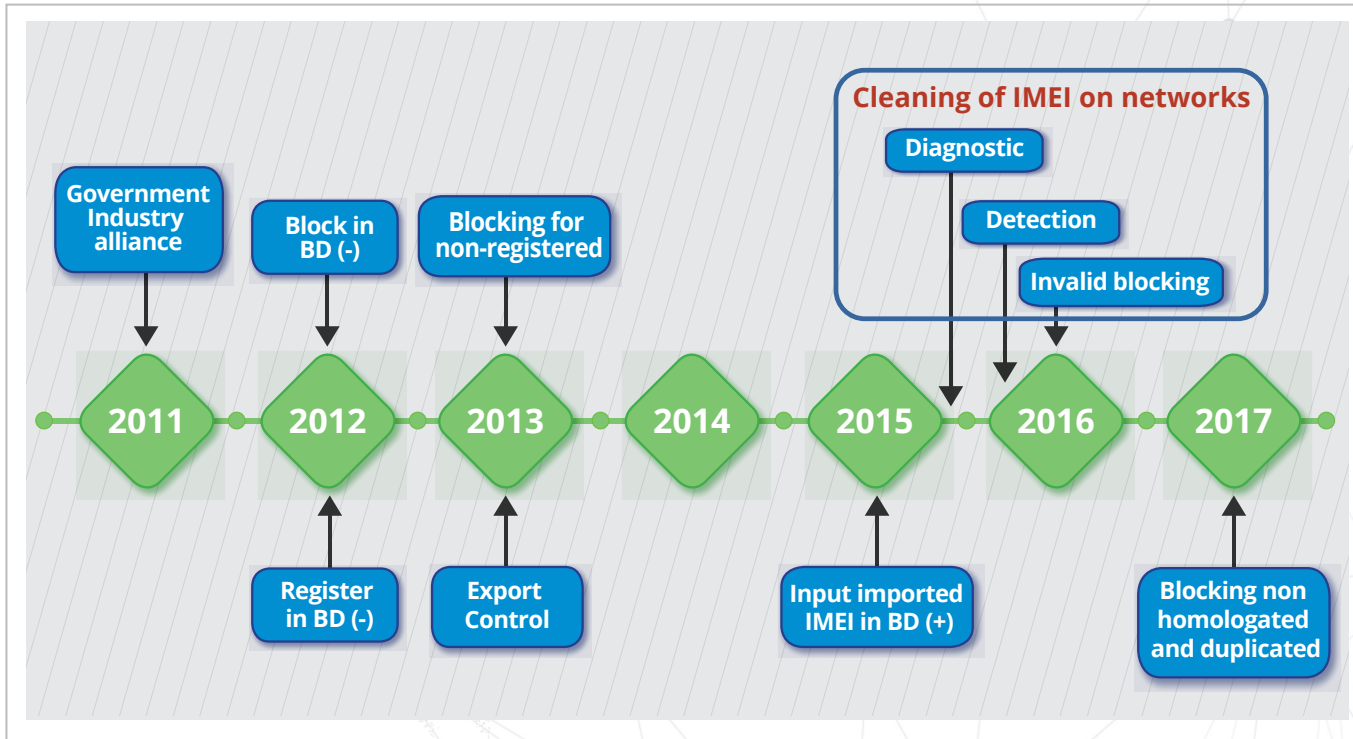


Source: CRC



The figure 3 shows the timeline of the adoption of the different IMEI control phases.

FIGURE 3



Source: CRC

Figure 4 shows the dates of the beginning for each type of control.

FIGURE 4

	MAY-2013	OCT-2016	FEB-2017	MAY-2017	OCT-2017
Not registered	█	█	█	█	█
Not valid		█	█	█	█
With no format			█	█	█
Non-homologated	█	█	█	█	█
Duplicated					█

Source: CRC

The time that the phones can be blocked also depends on the category of phone issue being addressed as follows in Table 3.

TABLE 3

Colombia IMEI-Blocking Scenarios

IMEI Scenario	Grace period before phone's IMEI can be blocked
IMEI with incorrect format	These can no longer be connected to Colombian mobile networks
Invalid IMEI that was not allocated by GSMA	30 days (As of March 15, 2018, will be reduced to 2 days)
Non-homologated phone	90 days (As of March 15, 2018, will be reduced to 45 days)
Duplicated IMEI	30 days
Not registered in the 'positive' database list	20 days
Phone reported as lost/stolen by user (has been in effect since January 2012).	25 minutes

Source: CRC

The Role of the Consumer

Like any successful, large-scale solution that impacts large swaths of the country, working closely with other government agencies was critical. MINTIC took a highly visible stance to explain to consumers why the registering of their phones was something that would lead to positive results. Through the website nomascelusrobados.com (the equivalent of 'nomorestolenphones.com' in Spanish) consumers are given sufficient information on the purpose, process, and value of the system being implemented.

While more advanced users may be able to find the IMEI of their phone with limited effort, the educational and technological levels of all the consumers in a country can vary greatly requiring solutions be as user friendly as possible. Typing `*#06#` is a universal method adopted by all mobile phone manufacturers to allow users to identify the IMEI number of their phones. On the [nomascelusrobados](http://nomascelusrobados.com) website, consumers also have links to the nine mobile operators (both traditional and MVNOs) with easy to follow step-by-step instructions for how to register their phones. In addition, the mobile operator that receives the report of a lost/stolen mobile device from its user, is obligated to determine the IMEI that had activity in the network on the date and hour of the theft, to precisely block the correct IMEI.

The CRC website is easy to navigate for users that might not be technically savvy as seen in Figure 5:



Note: This is a translation to English by IDC of the CRC Website.

Source: <https://www.crcm.gov.co/es/pagina/medidas-contras-el-hurto-de-celulares>

The landing page has clear areas to perform tasks such as:

- See more information about how to register your phone.
- Review lists of homologated phones.
- Learn how to homologate your phone (accompanied by a step-by-step video detailing the process).
- Understand the process for reporting a stolen phone.
- Download forms for registering phones, transferring used phones to other users, and when needing to resolve a duplicate IMEI issue.
- Reviewing the list of businesses authorized to sell mobile phones in Colombia.

Customers are contacted by all means possible, at a minimum by SMS, and via additional methods such as phone calls, and email, among others. The SMS messages sent to the Colombian users with handsets with duplicate IMEIs alerts them as follows: "The IMEI for your phone is duplicated and could be blocked. Present to your operator the purchasing documentation within the next 30 calendar days"⁷ In a similar fashion, there are appropriate SMS for users of phones with IMEIs that are invalid, non-homologated or not registered.

⁷ Original Spanish: "El IMEI de su equipo está duplicado y podría ser bloqueado. Presente ante su operador el equipo y sus soportes de compra o adquisición"

Since many customers might not be aware that the phone they are using is irregular or not homologated, it would be unfair to cut off their phone service without a proper awareness campaign and amnesty program. It is the regulator and operators' responsibility to execute an effective ecosystem awareness campaign before, during, and after implementation to ensure all parties — distributors, retailers, and especially consumers — are aware of the new system, timelines, purpose, processes, risks, benefits, and other key information. After being properly educated, it is the consumers' responsibility to ensure they take the appropriate steps before purchasing a new phone or risk being blocked.

Industry Involvement

The mobile operators' physical retail locations or independent retailers can also play a critical role in helping diminish the instances of stolen or irregular phones. Once the phone is in hand, the agent can quite easily perform the following quality control activities and quickly identify a phone that should not be allowed service:

1. Confirm if the IMEI is included in the negative database through a query of a public web page.
2. Confirm that the IMEI number printed on the sticker for the phone matches with the IMEI number that is generated from the phone itself when typing *#06#.
3. There could also be obvious signs of questionable devices if the packaging materials look suspicious, phone's physical appearance is not correct, logos are altered or missing, etc.
4. If the customer happens to have a receipt for the phone, check whether the information on the receipt regarding brand, model, color, or IMEI matches with the phone being presented and it's legitimate.

Control and handling of a phone with a duplicated IMEI

On a daily basis each mobile operator, based on the voice CDRs⁸, can detect duplicated IMEIs using algorithms to identify collisions or time/distance conflicts between the calls placed from different IMSIs⁹ with the same IMEI. In the same manner with the same kind of algorithms, a centralized monthly system detects duplicated IMEIs showing activity in different networks at a national level. Once detected, they identify

8. Call Detail Record. It is a data record produced by a telephone that documents the details of phone calls.

9. International Mobile Subscriber Identity. A unique ID code for each mobile, included in the SIM card.

the IMSIs that have been using the duplicated IMEI and its users are alerted and given 30 calendar days to present (physically or virtually) the purchase documents related to the phone, plus information about the point of sale and other personal information. This information is delivered to law enforcement to investigate the crime of IMEI tampering.

At the end of the grace period in which the users of phones with duplicated IMEI supply the required information and supporting materials, the mobile operator in which the phone is being used must apply the criteria set for in the regulation to define which of the users can continue to use the equipment.

There are two criteria for the operators to define which user can continue to use a phone with a duplicated IMEI:

1. The user that has registered the IMEI under his ID, or
2. The user whose supporting materials or phone provide the operator with enough evidence that the phone is the genuine one.

Once the user of the legitimate device, with the above criteria, has been identified, the mobile operator will associate the correct IMEI-IMSI coupling in its EIR to only allow access to the network the phone that attempts to use the IMEI with that IMSI. In this way the duplicates are blocked. The (single) IMEI is placed in the centralized negative database for identification purposes to users, other operators and authorities.



Stolen Phone Handling

In the case of a phone being reported as stolen, the process is much simpler. The user is required to immediately report the theft to his or her mobile operator and should formally report it to police or legal authorities. However, only a very small percentage (no more than 2%) of the phones stolen in Colombia are reported to local police authorities. In most cases the person will call the mobile operator themselves to report the phone as being stolen, at which point the details on the phone, IMEI (taken from the network activity by the date and hour of the theft), and customer details will be placed into the system to have the IMEI blocked in less than half an hour.

The stolen/lost reported IMEIs received by the mobile operator are shared on-line to the centralized negative database and the IMEI is broadcast to the rest of the mobile network operators to be blocked in a maximum time of 25 minutes. By regulation, information about the theft must be populated in the negative database, such as the address/location of the event, if there was violence involved, if there were weapons involved, if the victim is a minor and contact information. With this information, law enforcement and judicial authorities can start investigations in the absence of the formal report from users, perform geospatial analysis of the hot spots of criminal activity involving stolen phones to reinforce the surveillance in those areas, and arrest thieves or people receiving stolen phones.

Homologation Process

The process for homologating a new phone model for the Colombian networks is a straight-forward process that is submitted to the CRC for both individuals and manufacturers or importers. After speaking with a phone manufacturer who recently went through the process, IDC can confirm that

the approval can be completed in less than two weeks. Since Colombia's mobile networks use the same 850 and 1900 MHz bands that the majority of the countries in North, Central, and South America use, most phones that are coming to Colombia already have regulatory approval from the Federal Communications Commission (FCC) in the USA. This helps speed up the process immensely since the network compliance issues have already been confirmed. Since August 2016, MINTIC has waived the fee for this approval process in Colombia. In those cases where an importer or manufacturer wants to sell a new phone model that has not been approved by the FCC, then the company or individual applying for the approval would be responsible for paying the costs associated with the independent, government recognized laboratories who perform this kind of analysis.

In the process of homologation, the applicant must present the TAC allocation certification for the CRC to validate the integrity and validity of the new model identification accordingly with industry standards through access to the GSMA database. Once homologated, the trademark and model are publicized in the CRC web page for the public to see the homologated phones that can be sold and used in the country. At the same time, all TACs related to the model are pulled out from the GSMA database and placed in a confidential list of trademark-model-TAC, which allows the mobile operators to detect daily which of the IMEI with activity in the networks belongs to a non-homologated model and inform the user and give them a grace period to homologate the phone with the CRC. As a result of this control initiated in October 2016, approximately 22% of the handsets presented to CRC by users for the homologation review resulted in identifying lost/stolen phones that were tampered with to alter the original IMEI with IMEIs that are not sold in the country or region.

Personal Imports

As a transition at the beginning of the control of non-homologated phones in October 2016, there was a process in place for individuals who had phones before the regulation was enacted and that they may have purchased overseas or in a questionable sales channel to make sure it was homologated. Via social media campaigns of #notequedesinmovil (#don'tbeleftimmobile as a

translation to English), users were directed to the www.notequedesinmovil.gov.co website. An example of an online pop-up can be seen in Figure 6. They were then instructed how to take the appropriate pictures of the IMEI stickers and other important identifying information like the FCC-ID which can all be uploaded to the website for a quick approval of no more than 10 business days. On their side, the CRC looked up the appropriate FCC certifications to homologate the model, if available. As of April 2017, the individual or company who is trying to have the phone homologated now needs to provide all the technical information themselves. A detailed video also helps applicants find the required information and explains the process for submitting it to the CRC.

FIGURE 6

Example of pop-up from crcom.gov.co website



Translation:

#NoTeQuedesSinMóvil = #DontStayImMobile

www.notequedesinmovil.gov.co

ESTE 1 DE MAYO = This May 1st

INICIA EL BLOQUEO DE CELULARES NO HOMOLOGADOS = Starts the blocking of non-homologated mobiles.

CONOCE EL PROCESO PARA HOMOLOGAR VISITANDO www.notequedesinmovil.gov.co = Learn about the

process to homologate at www.notequedesinmovil.gov.co

Source: CRC website

Near Term Results

Although the IMEI control system in Colombia (Figure 2) continues to be modified and enhanced, the CRC and local authorities have already begun to see very positive trends:

- Decrease in the number of stolen phones, especially in those cities where hot spots of thefts have been identified and police surveillance has been reinforced.
- Decrease in the number of phones with invalid IMEIs.
- Increase in the number of registered phones (legally imported and sold).
- Increase in the number of legally homologated phones.
- Decrease in duplicated IMEIs within the intra-network environment.

While initial results and implications are still being fully assessed, the costs of setting up and maintaining a system to categorize and block phones looks to have the potential to provide a multiplier effect of positive outcomes for all parties involved.

Below, in Table 4, are some of the recent blocking statistics reported by the CRC:

TABLE 4

CRC Results in Colombia from IMEI Blocking System

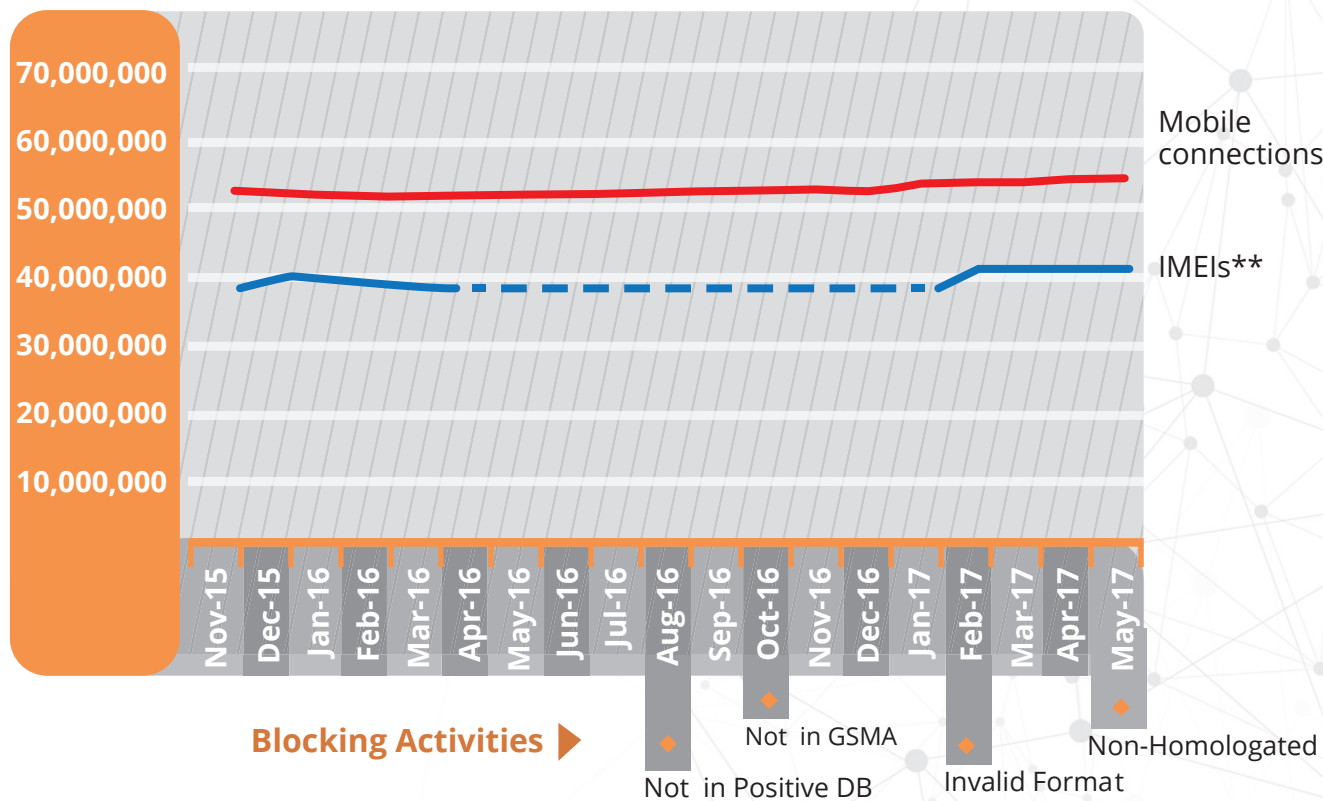
Type of IMEI	Total IMEI Impacted	Control Measure Taken
Incorrect Format	2.3 k	No access to the networks
Invalid	1.8 million	Permanently blocked
Non-homologated	1.8 million	Blocked, but can be reinstated once corrective actions taken
Not registered in positive database	6.1 million	Blocked, but can be reinstated once corrective actions taken
Duplicated	820 k	More than 2.5 Million users have been notified. On-going blocking procedures are in effect
Registered in Positive DB	134 Million	Since the beginning of database operations in 2012.

Source: CRC, as of December 31, 2017

As the figures show above, this system has had profound effects helping address illegal devices in a very short period of time (2016 and 2017). The immense success has caused some concern throughout the operator community about the potential implications blocking can have on subscribers, revenue, and other KPI's. While the results and implications will be market specific and highly dependent on implementation and governing rules the number of total phone lines has not been impacted negatively (Figure 7). This should help reassure the operator community that if deployed properly such systems can bring significant benefits that strengthen their business and help put them in a better position to support future traffic requirements.

FIGURE 7

Mobile Phone Subscriptions in Colombia



*Dotted line denotes estimates, full dataset was not available

Source: *GSMA Intelligence; **CRC

QUALCOMM'S ROLE IN HELPING THE ECOSYSTEM SOLVE THIS CHALLENGE

As a pioneer in the development of system-level, core technologies for the mobile industry for over three decades, Qualcomm has vast experience across the ecosystem and geographies. Whether working with handset manufacturers on the latest premium devices or engaging with network operators to ensure flawless network deployments, Qualcomm is an important partner for stakeholders across the mobile environment. Qualcomm understands that monitoring network and device performance is crucial, and for years has assigned engineering teams to engage with mobile operators throughout the world, including Latin America. Qualcomm consequently noted at an early stage the wide variations in device performance caused by sources such as design factors, component quality, antennas, and modem features, among others. After studying the issues, Qualcomm concluded that fraudulent and counterfeit devices cause a significantly higher prevalence of performance and network issues.

In Colombia, Qualcomm and the CRC jointly identified potential solutions and mechanisms available to specifically address the local challenges. Qualcomm consulted with the CRC as it defined the Colombian business rules for its IMEI control system. Once the most appropriate solution was identified by the CRC, Qualcomm developed a platform for device analytics with custom features tailored to CRC's needs. Qualcomm showed that it understands the importance of ongoing collaboration with its local partners as the dynamics of the market continuously change. For these reasons, regulators and telco operators across the globe consult with Qualcomm to gain from its expertise.



III. WHAT SHOULD THE REGULATORS BE DOING?

In addition to the Colombia IMEI control system which focused on stolen/tampered devices, fraudulent and counterfeit devices are a large and growing problem that needs to be addressed immediately with the right solution or we risk it growing to even greater proportions. Momentum is building globally in the fight against illegal devices and as other countries begin blocking, their illegal devices will likely flow into countries that don't have solutions in place, thus potentially putting even more pressure on an already challenging problem. In Latin America and other emerging market countries, the fact that the same solution that allows regulators to reduce the incidence of stolen phones can also eliminate the connection of fraudulent or counterfeit phones has ended up being a win-win for everyone involved, except for criminal organizations and illegitimate phone manufacturers.

So, what can and should regulators and other key stakeholders be doing now to ensure they are not one of those lagging markets that can become the last bastion for trade of illegal or stolen devices?

- **Engage with experienced subject matter experts:** There is no need to 'reinvent the wheel' when it comes to implementing solutions to reduce or eliminate these fraudulent or stolen phones from the networks. Mobile systems experts such as Qualcomm have teams of experts across the globe focused on helping regulators ensure the processes and rules in place are best in class and most appropriate for what the regulators or governments are trying to achieve. There are also regulators, like the CRC in Colombia, with success stories who are open to explaining their programs and helping others in their migration to fraudulent IMEI-blocking solutions.
- **Access and quantify the issue:** Working closely together with law enforcement, customs, telco operators, and handset manufacturers, regulators are uniquely positioned to most efficiently serve as a 'clearinghouse' of data when it comes to the size and impact that fraudulent and stolen phones are having within a country's borders.
- **Implement a solution:** Implementing a technology platform or system that can adapt to changing conditions and is capable of monitoring active devices connecting to the network is crucial, that together with a legal database which validates entries with an official identifying system (such as GSMA for GSM technology) will allow for differentiating between the devices to take decisions related to controls and blocking. Unsophisticated or temporary solutions are simply not capable of combating the criminal enterprises involved in manufacturing and distributing fraudulent handsets

and thus it is important to ensure a comprehensive end-to-end solution is implemented.

- **Launch consumer awareness campaigns:** As highlighted in the case of the CRC in Colombia, a well thought out consumer awareness campaign is critical in educating sellers and consumers on the risks of fraudulent and stolen devices and helping those consumers understand how to ensure the phones they purchase are legitimate.
- **Work with other regional or neighboring entities:** To have a greater and more lasting impact in helping combat fraudulent, counterfeit, and stolen mobile phones connecting to the networks, regional or global coordination for innovative solutions like that enacted in Colombia are beneficial. In a world of global commerce, blocking telephones in a single country may result in shifting the sale of those illegitimate phones to other countries where a solution is not in place. Working with regional entities tasked with harmonizing initiatives across geographies and throughout the ecosystem can help ensure that efforts are not isolated and are able to fit within a larger framework. Coordination between regulators in neighboring countries can also create a regional solution to the problem.

Together with the IMEI-control system, the successful consumer and ecosystem campaigns that the CRC has spearheaded in Colombia can serve as an example for other regulators in Latin America or other regions to follow. The importance of mass communications, ease of use for consumers or channel partners to check the status of an IMEI, and public service communications about the benefits the consumers and country will see as a result of implementing a solution such as the one in Colombia can all be used as a successful case study.

One of the regulator's primary responsibilities in every country is to protect consumers, and this is as important now as it has ever been. Citizen security and safety, among many other factors, is being put at risk by the continued growth of fraudulent, counterfeit, and stolen devices, and it is the regulator's obligation to take appropriate action. Effective solutions are available today; you can reach out to industry subject matter experts such as Qualcomm to begin discussing the most appropriate solution for your country.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries.

IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

To learn more about IDC, please visit www.idc.com.

Follow IDC on Twitter at @IDC.

IDC Latin America

4090 NW 97th
Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com

Created by



Sponsored by



Copyright notice

This publication was produced by IDC Latin America Integrated Marketing Programs. The results of opinion, analysis, and research presented therein were obtained from independent research and analysis previously conducted and published by IDC, unless sponsorship by a particular provider is otherwise specified. IDC provides IDC content in a wide variety of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of the licensee or its opinion.

Copyright © 2018 IDC. Total or partial reproduction, by any means or form, is prohibited without the express written consent of the owner.