Global Best Practices in Combating Mobile Device Counterfeiting

iconectiv™

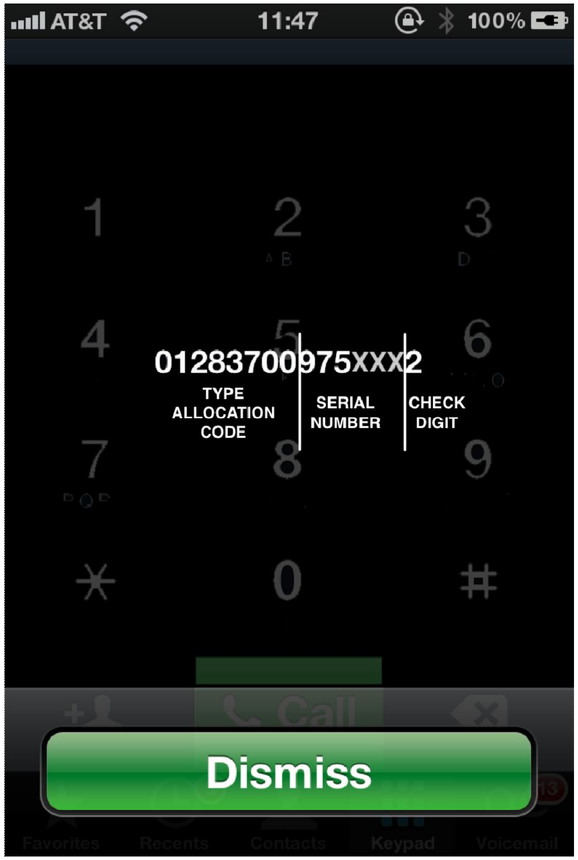
experience
performance
results

Timothy Jasionowski
Vice President
Product Management

tjasionowski@iconectiv.com
+1 781 775 3080

Basics of Device Identification: IMEI

International Mobile Equipment Identity



GSM 03.03 standardized the IMEI format to 15 digits. The format is structured as follows:

Type Allocation Code (TAC):	8 digits
Serial Number (SNR):	6 digits
Spare (SP):	1 digit

Represents a globally unique device and configuration

- In this case, TAC 01283700 is a black US Market AT&T iPhone 4 with 32GB
- Multiple TAC ranges may be assigned to the same device depending on volume of device sales and other manufacturer requirements

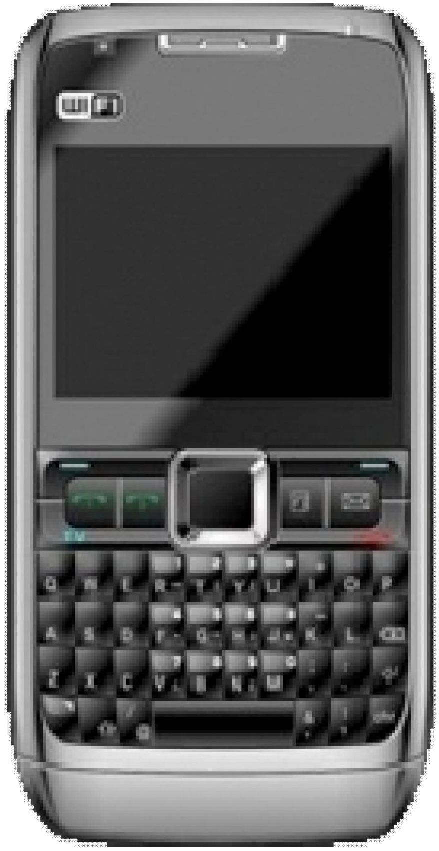
Identifies the device throughout the supply chain

- Distributor records, importation declarations and other channel management solutions use IMEI to denote specific devices
- May resolve to other manufacturer IDs

2010: 2G Knockoffs of Modern Devices

- Nokia E71
- Symbian 3.1
- Single SIM
- 3G/2G
- 801.11b/g
- Symbian Browser
- Mail for Exchange

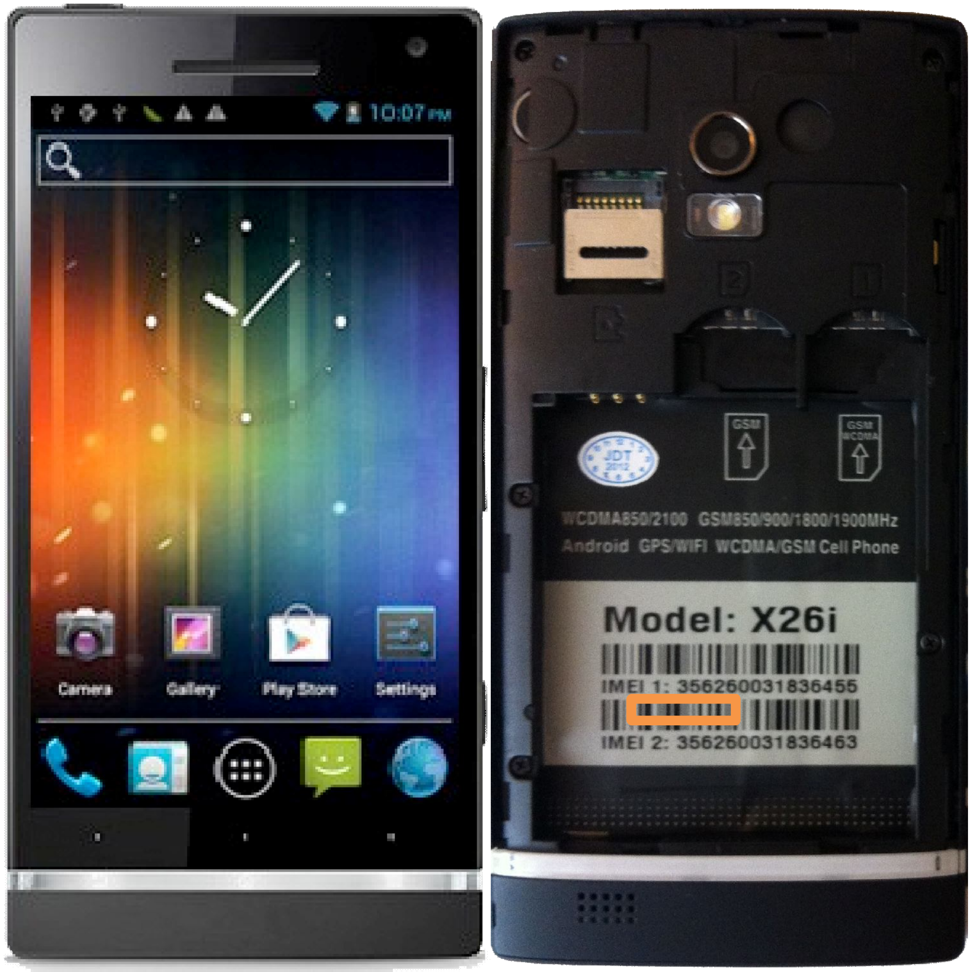
- 2012 Street Price: $260



- Chang Jiang E71
- Touch Screen
- Java Phone
- Dual SIM
- 2G
- 802.11b/g
- Opera Browser
- Facebook
- Analog TV

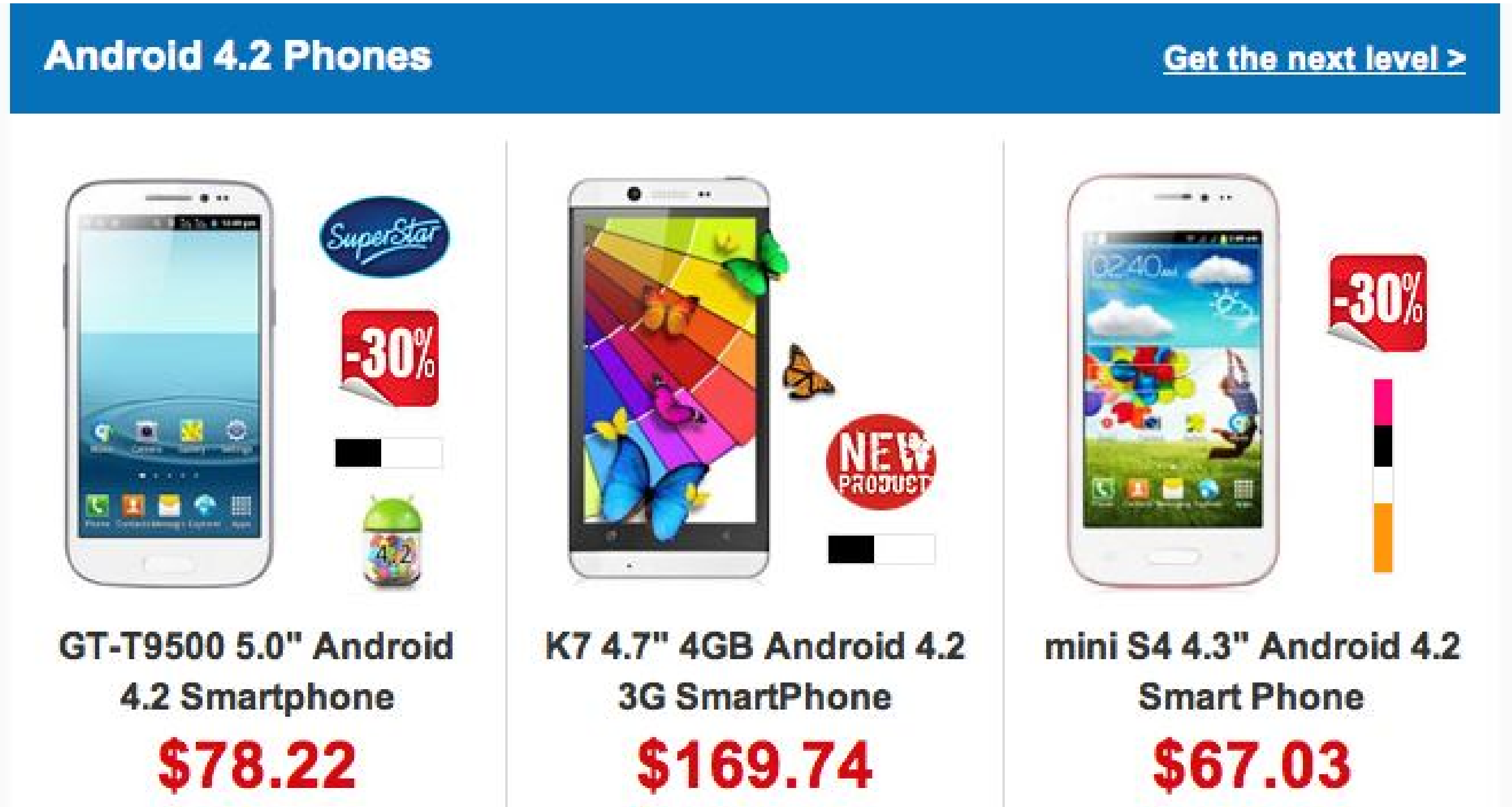
2012 Street Price: $40-60

2012: Modern 3G Android Counterfeit



- Purchased August 2012
- Sold as Star X26i
- MediaTek MT6575 1Ghz Chipset
- Dual SIM
- GSM:850/900/1800/1900 MHz
- WCDMA:900/2100 MHz
- Android 4.0.3 (Ice Cream Sandwich)
- Duplicates a Legitimate Device IMEI
  - Claimed Type Allocation Code: 35626003
  - Cheng Uwei Precision Industry
  - Model OX-11
  - GMS:900/1800 MHz
- IMEIs Pass Luhn Check
- Market Price in Hong Kong: US$150
- Wholesale Price: <$115 (estimated)

2013: Economy of Scale



Android 4.2 Phones

Get the next level >

GT-T9500 5.0" Android 4.2 Smartphone

$78.22

K7 4.7" 4GB Android 4.2 3G SmartPhone

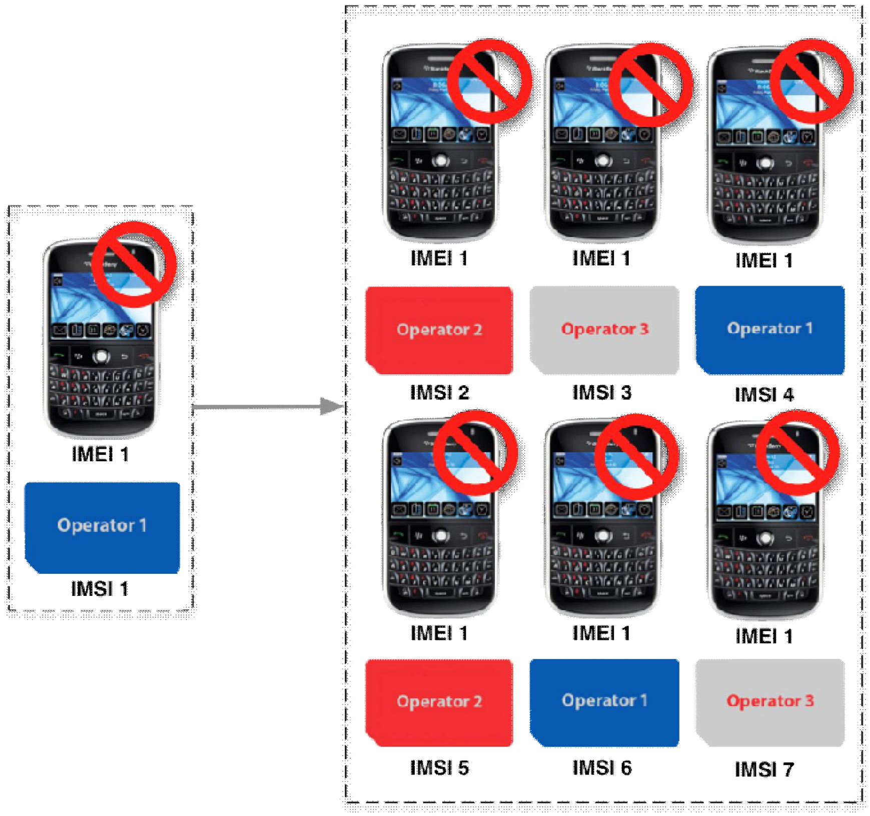
$169.74

mini S4 4.3" Android 4.2 Smart Phone

$67.03

Traditional IMEI-based Blocking No Longer Works

Use Case Example: Theft Involving Phone with Replicated IMEI



- By design, IMEIs should be globally unique and assigned to a single manufactured phone
- Illicit manufacturers and reprogrammers ignore this convention and either utilize legitimate IMEI data or simply put no IMEI number into the phone at all
- If ranges are reused or reprogramming is done blindly, the action of blocking one IMEI number in an operator EIR could block thousands of mobile devices accidentally
- Systematic management of cloned devices is better for the consumer and the operator
  - Blocked phones can not generate revenue during transition
  - Lack of transparency, notification leads to consumer confusion when actions are taken
  - Poor user experience (call drops, handoff failures) of counterfeit, uncertified phones

The Impact of Mobile Device Counterfeiting

Mobile Device Counterfeiting is an Economic Problem

- Users will always look for the best value in purchasing a mobile device
- High FRAND costs for 3G and LTE devices will create a perpetual advantage for counterfeiters
- Counterfeiting, cloning, smuggling and theft undermines legitimate resellers and domestic manufacturers of mobile devices
- Systematic, unmanaged blocking aggravates citizens while undermining operator ARPU

Mobile Phone Smuggling Undermines Source of Revenue for Governments

- Mobile devices have high import duties, VAT/GST receipts
- Counterfeit mobile devices lack unique IMEI numbers, making customs enforcement and reconciliation at PoS, at operator or in supply chain difficult
- Smuggling, customs fraud undermines domestic manufacturing incentives

Counterfeit, Uncertified Phones are a Threat to Domestic Mobile Networks

- Illicit devices generally have higher call drop rates, tower handoff failures and contribute to poor mobile network performance for all subscribers
- Loss of certification, testing revenue to regulator, undermining mission

Solution Success Vectors

This is not a simple clearinghouse, it is an evolving model

- Fixed databases will not solve this problem
- Illicit activities will always adjust to the introduction of new countermeasures
- Like anti-virus software, systems must be able to absorb new information, adjust to new threats

This requires cooperation between commercial concerns

- Manufacturers, operators, importers and government must work together to combat these issues

This process can and should be monetized

- There is money to be recaptured through national mobile device management
- Long term benefit is pushing legitimate devices through official channels

Mobile Phones and Key National Policies

Theft

Rising mobile devices average selling prices, fluid resale markets driving device theft and, in many cases, injury or death associated with the act

Terrorism and Organized Crime

Mobile phones increasingly used in the planning and execution of terrorist and criminal acts, including kidnapping and improvised explosive device (IED) triggering

Smuggling and Greymarket

Greymarket importation of mobile devices, underground market channels undermining government collection of import duties and GST/VAT

Counterfeiting and Cloning

Uncertified and unregulated mobile devices undermines legitimate, regulated manufactures and national industrial policies, lowers tax receipts, and deteriorating mobile network performance

Best Practice: National Device Registries

A unified, national infrastructure for management of mobile equipment

- Apply a single economic operating model over a nation’s mobile equipment ecosystem
- Act as cross-operator scheme to collect, analyze and act against a variety of mobile network-based threats
- Focus on tracking, modifying and managing consumer behavior over time
- Implement a common, automated data collection scheme across operators
- Enables cross-Operator and cross-Manfuacturer analytics and reporting while maintaining structural separation of data

A platform that adapts to new and changing threats

- Track and correlate devices, subscribers and roaming mobiles across all mobile networks on a common timeline
- Provide a common enforcement regime to detect, react and discourage theft, smuggling and counterfeiting
- Create a source of new data to combat terrorism, espionage and organized crime
- Adapt and evolve over time to address ongoing and emerging threats

Thank You!

iconectiv™

experience
performance
results

Timothy Jasionowski
Vice President
Product Management

tjasionowski@iconectiv.com
+1 781 775 3080