

Techniques used by cheaters to bypass the systems of control and registration

Evgeny Zababurin, SC.Soft LLP, Kazakhstan





The problem

- Governments lose out on unpaid tax
- Industry worldwide loses a lot because of counterfeiters
- Consumers receive poor-quality goods often at an excessive price
- Counterfeit often appears in other criminal activities (kidnapping, drugs, money laundering, and terrorism)

How counterfeit or
illegal devices are used
for criminal purposes

Methods used at manufacturing phase

Counterfeiters produce and sell expensive, low-quality equipment under the guise of well-known brands.

The most copied brand by fake phone makers: Samsung, Apple, Huawei, Xiaomi, Oppo, and Honor.



1: GSMA Type Approval process not respected

Equipment manufacturers either do **not go through GSMA type approval** or do it at a very low cost.

Paths available:

- Use someone else's TAC code for their batches of devices.
- Using a single IMEI code for the whole batch of devices.
- Using one TAC code (even their own) for different models.
- Using TAC codes not assigned by anyone.
- Using the same IMEI in different slots of the same device.

2: Use lower quality components

Some manufacturers may use lower quality components to save money, which can lead to poor quality products and increased costs associated with scrap, rework, and warranty claims



3: Do not provide warranty services

Lack of transparency and accountability in the cell phone industry allows for practices that may negatively impact consumers and the industry as a whole to continue.

SORRY

No
Guarantee
No
Warranty
No
Return

Methods of traders / importers

1. Avoid device certification with telecom regulators
2. Avoid customs clearance
3. Avoid registration of modular devices where required
4. IMEI Authenticity

1: Avoid device certification with telecom regulators

For certification, an official, genuine device is submitted. It passes inspection and is issued with a certificate.

Counterfeit units are then imported using the same certificate. The manufacturer and model are claimed to be the same. In reality, however, their quality and characteristics are not respected.



2: Avoid customs clearance

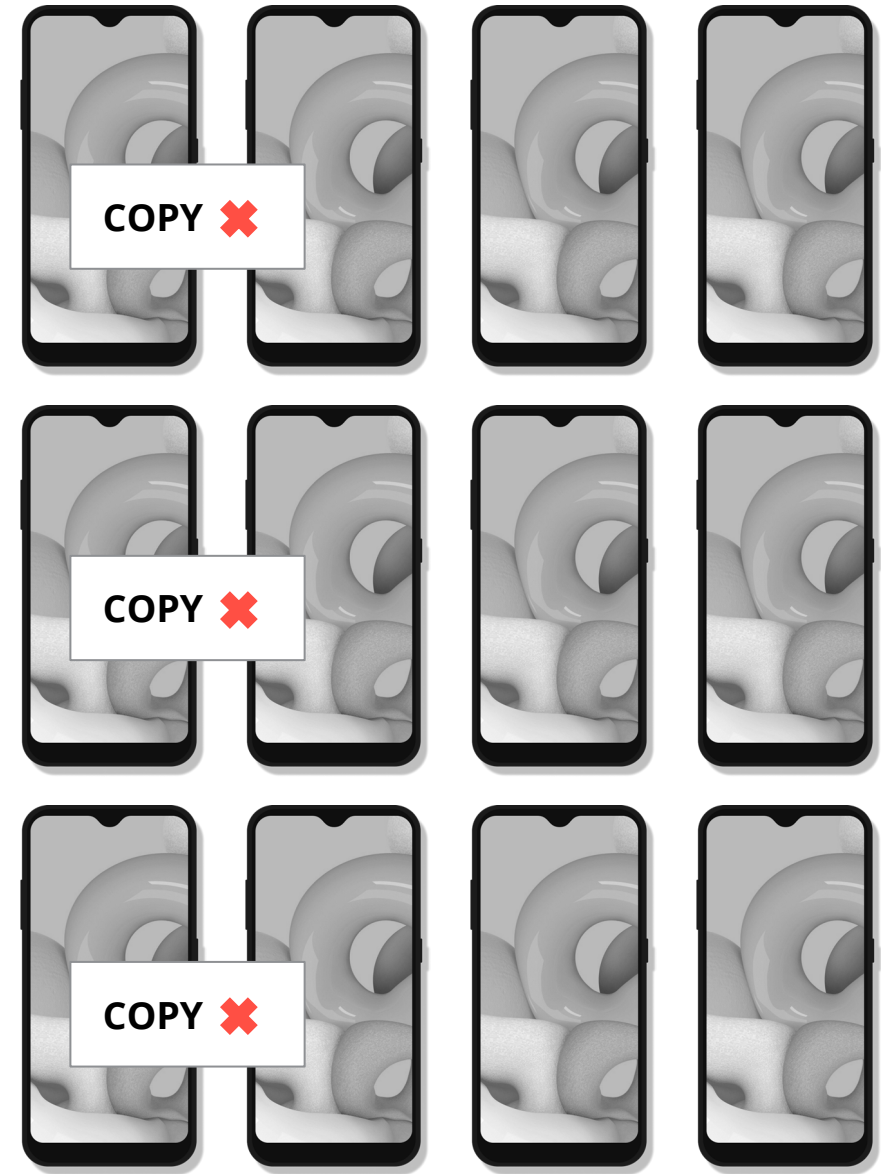
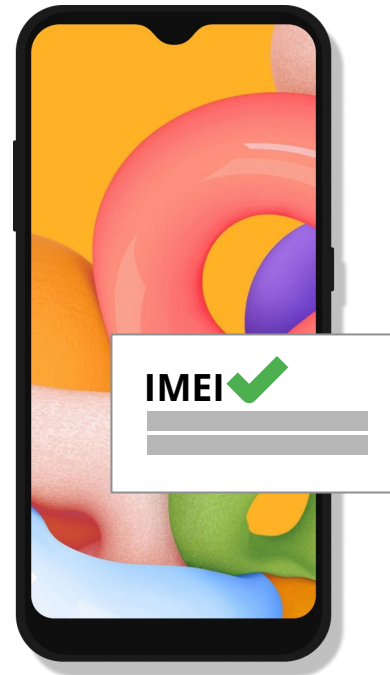
- Individuals bring in small batches, bribe customs if caught
- Change Customs code and Import as another product (e.g. spare parts), especially for M2M, IoT devices
- SIM boxes/farms likely never certified, so import as something else

3: Avoid registration of modular devices even if required

- Avoid registration, put it to the end-user
- Only register one IMEI in multi-SIM devices
- Steal passport data of recent arrivals for registration
- Duplicate IMEIs create problems for buyers and the government;

4: IMEI Authenticity

A single IMEI is legally imported and registered. Then a batch of devices with the same IMEI is smuggled into the country.

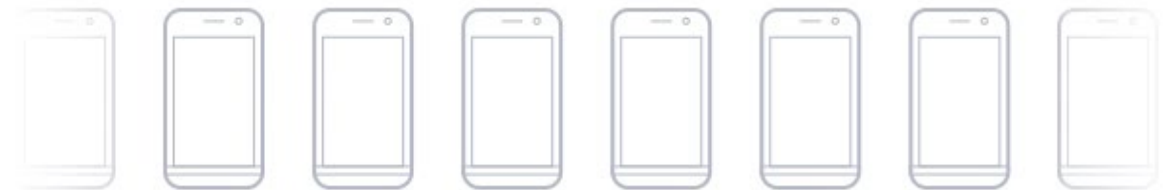
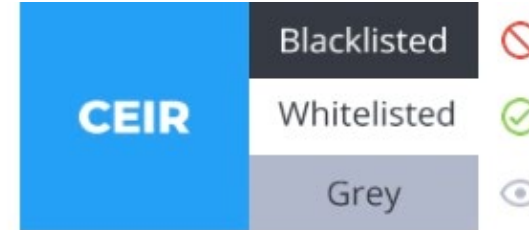


How to deal with these issues

- Sending a one-time code to the applicant to verify that the number provided is their own.
- Use FaceID technology to verify that the applicant has provided their passport details.
- Automated verification of the applicant's ownership of the number provided by the mobile operator's IT systems.
- Automated verification of the person's date of entry into the country by the border guard's IT system.
- A public portal where the buyer can check the IMEI of the device before purchase (whether it requires registration or not, etc.).

Solutions

- Unified registry of allowed IMEI codes at national and international levels
- Automated detection of unauthorized devices
- Blocking unregistered devices by operators
- Integration with government bodies and financial sector



Conclusions

- International cooperation is key to combating the spread of counterfeit devices
- A comprehensive approach will minimize damage from counterfeits for all market players





Techniques used by fraudsters to bypass the systems of control and registration

Evgeny Zababurin, SC.Soft LLP
2023

 soft.sc

 product@soft.sc