Contribution of Wind Tre
to
BEREC Stakeholder Workshop on Combating Fraud
Brussels 21 May 2026

Antongiulio Lombardi

Regulatory Affairs Director

Wind Tre

Giovanni Broccatelli

Head of Core and Beyond the Core regulated Markets

Wind Tre

Agenda

1	The methodology
2	Anti-Spoofing Solution
3	Sim-Swap Solution
4	Conclusion

The working method developed by AGCOM to identify solutions to complex problems (1/2)

- The identification of technical solutions to complex problems in Italy has been possible thanks to a working method that AGCOM has developed, and which is based on a structured discussion with operators in the digital sector.
- We believe that the approach makes it possible to balance decision-making autonomy on the one hand and technical understanding of the phenomena through the active and continuous involvement of operators.
- This makes it possible to define regulations which, in terms of effect and effectiveness, exceed what can be done with individual public consultations or individual hearings.
- The method does not reduce the clear separation that must exist between the role of the regulator and the regulated economic entities but allows a complete acquisition of all the elements relating to the specific problem through consultation with the operators and leaves the decision to AGCOM in the full exercise of its powers.

The working method developed by AGCOM to identify solutions to complex problems (2/2)

The method used by AGCOM can be summarized as follows:

1. AGCOM's observation of particular phenomena
2. Launch of initial discussions with operators on specific technical tables
3. Definition of clear regulatory indications of principle to guide subsequent work following one or more public consultations if necessary
4. A subsequent phase of structured discussion with operators and with the Industry (technical tables) in general to analyze the technical limits, objective constraints and real possibilities of intervention.
5. Finally, in full respect of the competences, a final decision is taken by AGCOM, aware of the overall framework and operational implications.

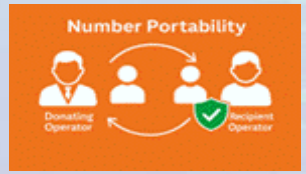
Relevant areas in which AGCOM has used this approach

Counter to SIM-Swaps

Anti-Spoofing solution

Combating audiovisual piracy through the introduction of the Piracy Shield

Protection of minors, with the generalized introduction of parental control



Definition of migration procedures and number portability in the fixed and Mobile Number portability in mobile.

Anti-spoofing solution identified by AGCOM in Italy
The AGCOM model at a glance and why it works

Structured collaboration

AGCOM uses technical tables for continuous discussion with operators, integrating regulatory and industry technical skills.

Informed decision-making autonomy

AGCOM maintains autonomy in decisions, benefiting from a deep understanding of the technical implications and limitations.

Going beyond traditional consultations

The model allows for dynamic and iterative analyses, improving effectiveness compared to traditional public consultations.

Effective applications

The AGCOM model is successfully applied to issues such as anti-spoofing, SIM-swapping, the fight against piracy and the protection of minors.

Operator involvement

The direct involvement of operators guarantees feasible and sustainable solutions over time.

Pragmatic approach

The approach avoids ineffective theories, focusing on targeted and high-impact interventions.

Continuous adaptation

Constant comparison makes it possible to adapt the measures to technological and phenomenon evolution.

Trust and responsibility

The model fosters trust and shared responsibility between regulator and industry, protecting citizens.

Anti-spoofing solutions identified by AGCOM in Italy
The phenomenon of spoofing

- "Spoofing" refers to cases of calls in which the sender number is "altered" to avoid being identified.
- Used in the past to avoid paying symmetrical mobile termination rates by operators in non-European countries
- Used to make "robocalls" — automated phone calls, often fraudulent or advertising, with an altered sender number — which poses a growing risk to users' privacy and security.
- Robocalls have been joined by calls that are not automated but that exploit the same principle, the so-called "Spoofed calls".

- In general, it can be said that the phenomenon has various origins, but at the base of everything there is the intention on the part of certain subjects to make calls masking the origin of the call.
- The phenomenon is widespread worldwide and in various countries useful solutions to combat it have been studied or are being analyzed.

Anti-spoofing solutions identified by AGCOM in Italy
The path of Combating spoofing followed in Italy (1/2)

- The Italian solution starts from a cornerstone. the Italian Numbering Plan - Resolution 8/15/CIR and subsequent amendments and additions which
  a. prohibits Italian operators from originating calls to their customers having as CLI numbers other than those assigned by the operator to the customer's line.
  b. It prohibits Italian operators from altering the CLI when acting as transit operators.
- A customer of an Italian Operator cannot "Spoof" and if he does, he is identified
- In Italy, therefore, most calls with Altered CLI are conveyed through International Carriers. This element is also recognized in Recommendation ECC/REC/(23)03)
- In **2018**, AGCOM, with resolution 156/18/CIR, defined the obligation for Call Centers to ensure the presentation of calling line identification (CLI) and to ensure that the numbers used to make calls can be called back by the user.
- In **2019** , AGCOM, in the Anti-Fraud Technical Committee, launched a technical working group with the Operators to explore the applicable solutions, aware that Italian operators:
  - They can control calls originating from their networks
  - but they are not able to control the calls that are delivered to them by other operators.
- The issue is delicate: Blocking calls is an activity to be done carefully
- The Anti-Fraud Technical Table explored anti-spoofing and SIM swap solutions and in 2021 merged into *the "Committee for the Security of Electronic Communications*" established by AGCOM and which also sees the participation of the Postal Police and MIMIT.
- In May 2022, *the Committee for the Security of Electronic Communications* managed by AGCOM defined a shortlist of applicable solutions:
  - Blocking of incoming calls from international interconnections and having a CLI (fixed)
  - Blocking of incoming calls from international interconnections and having a CLI, an Italian mobile number, if the mobile phone is not roaming
  - Blocking of incoming calls from international interconnections and having a CLI an Italian number other than a mobile number (considering that outside Italy only Italian mobile numbers can originate in the event that the customer is roaming)

The proposals require technical discussion with operators

Anti-spoofing solutions identified by AGCOM in Italy
The path of combating spoofing followed in Italy (2/2)

- AGCOM in July 2022, allowed Italian operators on a voluntary basis to block incoming calls from international interconnections and having a CLI that does not adhere to the ITU T E.164 technical specifications
- Wind Tre was the first Italian operator to implement this measure in the first months of 2023.
- AGCOM did not make any other mandates as in 2022 it did not have the powers to impose the blocking restrictions.
- In 2023, AGCOM, with resolution 197/23/CONS, approved a Code of Conduct for Call Centre activities, introducing the prohibition of modifying the CLI not only for operators (for whom it had already been established by the PNN) but also for entities that carry out call centre activities for teleselling and telemarketing
- Also in 2023, AGCOM issued resolution 12/23/CIR which regulates the sending of SMS with ALIAS (i.e. having an alphanumeric sender as CLI) by introducing the obligation to block SMS with Alphanumeric Alias entering from abroad.
- AGCOM participated in the activities of the European Conference of Postal and Telecommunications Administrations (CEPT), aimed at the adoption of a specific recommendation and collaborated with the regulatory authorities of other European countries.
- In 2023, the Recommendation ECC/REC/(23)03 was issued, which contains a list of applicable solutions to combat Spoofing, including the basic principles already identified by AGCOM in 2022.
- In 2024, an amendment to the Electronic Communications Code introduced by Legislative Decree 48/2024 which provided AGCOM with the powers to work on blocking solutions:

  "2. [..] ***The Authority may establish rules of generalised application to block access from numbers or services in order to combat fraud or abuse, including by providing for dissuasive regulatory measures. In particular, the Authority may impose rules on entities authorised to provide electronic communications networks or services to block communications from abroad that unlawfully use national numbers to identify their origin, or that do not comply with the specific Recommendations of the ITU-T.*** *[..]."*

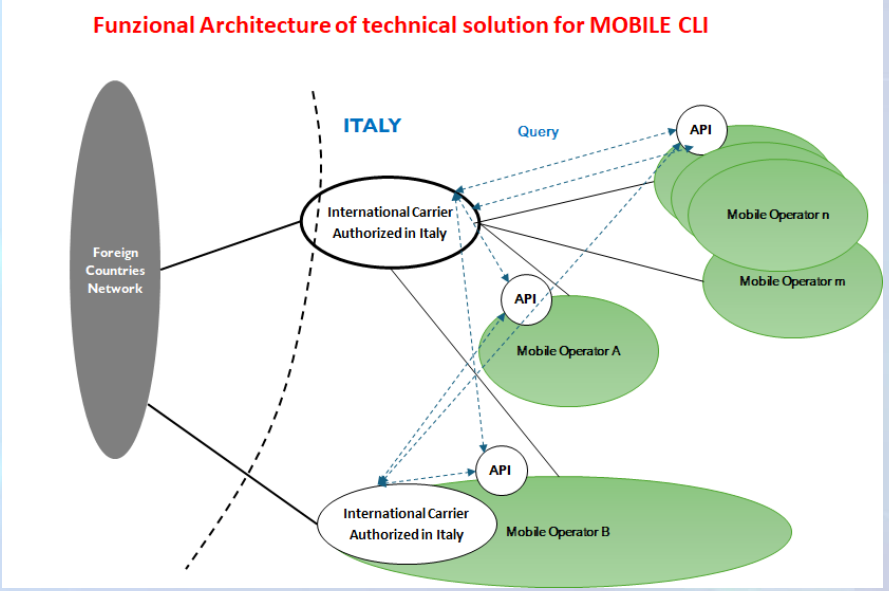
- In December 2024, AGCOM launched a public consultation (457/24/CONS) where it identified and submitted for consultation the anti-spoofing solutions that can be used, also launching a technical working group with operators to define the detailed technical specifications.
- The solutions identified and then regulated with Resolution 106/25/CONS at the beginning of 2026 aim to protect Italian customers at the "*border*" by preventing the entry of "Spoofed" calls and have been discussed and defined considering in detail all the necessary technical specificities.

Anti-spoofing solutions identified by AGCOM in Italy
The Italian Technical Solution

- The technical solution defined by AGCOM and contained in Annex A of Resolution 106/25/CONS provides in summary

    1. *Blocking of voice calls delivered by foreign operators that do not comply with the ITU Recommendations on numbering (ITU-T Rec. E.164 and E.157). Cases to be blocked – blocking of numbers that do not adhere to the ITU T.E.164 Recommendation and with a non-geographical but not mobile CLI*
    2. *Blocking of incoming international voice calls with valid national geographic CLI (CgPN for ISUP/TDM and PAI for VoIP).*
    3. *Blocking of incoming international voice calls with national mobile CLI (+393...) if the corresponding mobile customer is not roaming abroad.*

- Call blocking is carried out by Operators who act as "International Carriers Authorized in Italy", i.e. they are the so-called Border Operators, i.e. the national Operators who have direct relations with foreign Operators not Authorized in Italy.
- The type 1 and 2 blocks were implemented in August 2025 and do not require interaction of the International Carriers Authorized in Italy with other national operators.
- Type 3 blocks were implemented in November 2025 and provide for interactions between International Carriers Authorized in Italy and Italian Mobile Operators (MNO or Virtual) which are the only ones who know if a customer associated with a particular Mobile number is Roaming or not.



- In essence, in case 3 The Authorized International Carrier that receives a call from a foreign Operator with an Italian mobile CLI queries the Mobile Operator to which that number belongs.
- The mobile operator checks and returns to the Carrier an indication of Block or No Block.
- There is also a monthly report that all operators must send to AGCOM for the necessary checks.

Anti-spoofing solutions identified by AGCOM in Italy
The results

- The results of the solution were immediately evident.
- AGCOM, in a press release published on December 29 2025, highlighted the success of the initiative
  - **Between 19 and 30 November 2025, about 49.3 million** illicit calls from Italian mobile numbers were blocked, 4.1 million per day, equal to about **56% of the total calls from mobile networks with Italian numbers (about 88.3 million).**
  - Calls with an Italian mobile number went from a daily average of about 26.8 million, from 1 to 18 November, to a daily average of 7.4 million calls from 19 November to 30 November.
  - At the same time, calls with foreign numbers went from a daily average of 6.6 million (19% of the total), before 19 November, to 23.8 million (74% of the total), after 19 November.
  - 10 million calls from abroad with landline numbers were blocked.

		Calls from abroad with Italian mobile number (millions)	Calls with Italian mobile number blocked for spoofing (millions)	Calls with foreign numbers (millions)
Total	**From 1 to 18 november**	483,2	-	119,1
	From 19 to 30 november	88,3	49,3	285,5
Daily average	**From 1 to 18 november**	26,8	-	6,6
	From 19 to 30 november	7,4	4,1	23,8

- There are no more up-to-date official data on blocks at national level but as Wind Tre we can confirm that the phenomenon of calls from abroad with altered numbers has reduced but the most important thing is that at the moment calls with altered Italian numbers from abroad are blocked.
- A shift in illegal teleselling activities to numbers with a foreign area code has emerged, which are less effective as customers do not respond to these types of calls
- The remaining cases of spoofing with Italian numbers, duly reported to the Authority, are currently being monitored by AGCOM to identify the responsible parties, who can no longer hide behind the untraceability deriving from the use of a foreign operator.

Solutions to combat SIM swaps
Notes on the solution adopted in Italy (1/2)

Foreword

With regard to the problem of Sim Swap (the phenomenon of SIM replacement without the knowledge of the real holder) AGCOM has adopted a path similar to the one already illustrated.

The issue of combating SIM swaps arises within the Anti-Fraud Technical Committee where AGCOM has been addressing possible solutions to combat fraudulent SIM swaps together with operators since 2019 and 2020.

- The issue is addressed from two points of view:
  1. Possible interactions via API between Mobile Operators and banking institutions to carry out checks on the possible replacement of the SIM
  2. How to strengthen the measures for operators in the event of a request for a SIM change in the various cases (SIM replacement for theft, loss, breakdown or request for MNP)

The Next steps

- Solution 1, i.e. relations between Operators and banking institutions, is left to free negotiation between the various parties and there are solutions on the market that allow you to certify the SIM change.
- The issue of the SIM replacement request requested by an end customer from an operator is instead addressed by AGCOM starting from the regulatory bases and comparing with the market.
- It starts by considering that the Electronic Communications Code requires customer identification for: i) new mobile phone contracts, ii) contractual integrations and iii) number portability (MNP). This obligation also applies to online requests.
- However, it should be noted that there are no explicit identification obligations for some ancillary operations, such as SIM replacement (SIM deterioration, change of format - from physical SIM to eSIM, Theft or loss, etc.)
- In addition, the rules of MNP provided for the identification of the applicant but the data that was exchanged between the recipient and the Donating included the number to be carried (MSISDN) and the ICCID.
- Since the recipient Operator does not know the holder of the SIM at the Donating, a potential Fraudster can present himself to the Recipient with false documents, bring with him the Mobile Number on which to request portability and the ICCID and obtain a Portability or a SIM change, at least momentarily, i.e. until the real holder notices the fraud.

Solutions to combat SIM-Swapping
Overview of the solution adopted in Italy (2/2)

- During the work of the Anti-Fraud Technical Table, a significant increase in cases of unauthorized SIM replacement (SIM swap) has emerged, without the knowledge of the line holder
- Associated risks are of different nature:
  - bank fraud (e.g. access to home banking)
  - You can access:
    - Sensitive personal data
    - Other digital services
    - Use of data for further fraudulent activity

- AGCOM is therefore launching a public consultation aimed at defining the principles to be followed by operators in the event of a request by a customer for SIM Change, including cases of portability.
- The solution found by the Authority's resolution provides for the following general principles:
  - The recipient operator, in the event of a request for a SIM change, must identify the customer, and request a series of information such as i) identity document, ii) tax code, iii) copy of the SIM card (in the case of MNP or request for replacement due to failure or modernization) iv) copy of the report to the insurance authorities of theft or loss
  - Only the SIM holder can request the replacement of the SIM and no one else;
  - Among the information exchanged between Recipient and Donating are the mobile number to be brought and the tax code of the holder
  - The recipient must verify through a message to the number to be carried or to the number on the SIM to be replaced that the SIM is active and in the possession of the applicant for the replacement or the MNP.
  - The donor must reject the portability request if the tax code received does not match the one in its system
  - The takeover between two parties must always be carried out at the customer's operator in the presence of both the successor and the successor
- After AGCOM's general resolution published in 2021 (86/21/CIR) which also gave rise to the Committee for the Security of Electronic Communications, a table was launched between Operators to define in detail the specifications to be followed to implement the principles defined by the Authority.
- The technical table led by AGCOM and in the presence of the Operators meets numerous times and defines the various situations to be managed and the particular cases.
- The outcome of the technical working group was published by AGCOM (in April 2022) as a supplement to resolution 86/21/CIR which was originally published in July 2021.

The Outcome

- **The measures introduced have practically eliminated the cases of Sim Swaps and it is believed that the procedure adopted by AGCOM in comparison with the Operators has also produced excellent results in this case.**

Conclusion

Effectiveness of the solutions identified

- The anti-spoofing and anti-sim swap solution in Italy has significantly reduced the phenomenon by protecting users.

AGCOM governance model

- The AGCOM model is based on cooperation, technical expertise and regulatory progressivity, improving technology management.

Intelligent and collaborative control

- The Italian regulation demonstrates how a collaborative approach effectively addresses complex technological challenges.

Continuous Monitoring

- AGCOM's continuous monitoring of the phenomenon together with operators will make it possible to identify further needs.

Need for recognition of costs incurred by the Operators

- A legislative intervention is needed that recognizes the need to compensate operators for the burdens they bear to combat phenomena of public interest.