



Madrid, 10th April 2021

To whom it may concern,

Orange España Comunicaciones Fijas S.L.U. is a licensed operator in Spain fully owned by Orange Espagne S.A.U., a subsidiary of MasOrange S.L. which provides, among others, international voice services to wholesale customers around the world.

Our company is exclusively a transit carrier (intermediate service provider) that does not generate end-user traffic and is connected to hundreds of carriers worldwide.

Our company is not based in the US and we do not have the obligation to implement STIR/SHAKEN solution in our network. However, due to the nature of the services provided in our network, connected to carriers worldwide that could send traffic with destination in the US, you can find attached the different measures implemented to mitigate robocalls:

1. Compliance and Due diligence procedures

Our company has developed a robust compliance organization in each of our divisions, implementing our own specific Compliance and Fraud Due Diligence Methodology for identifying fraud and compliance risks related to third parties (suppliers, interconnect partners etc.). Since its initial deployment, it has constantly been improved by feedback from operational teams and fraud and compliance experts as well as requirements taken from relevant legislations and recommendations issued by Regulatory agencies.

Apart from the due diligence prior to sign any new contract with a carrier (updated/renewed periodically), all our contracts (with customer and providers) include relevant provisions to prevent any unlawful usage of the service, and giving us the right to immediately block any voice traffic that could be categorized as fraudulent.

Orange España Comunicaciones Fijas S.L.U. is a member of the i3Forum Fraud Fight workgroup, collaborating to define the guidelines for the international wholesale carrier community to fight against all types of fraud. Fraud clause in our contracts follows i3Forum guidelines.

2. Fraud management system

Our Fraud management system proactively monitors all traffic going through our network, detecting when certain predetermined thresholds are exceeded, sending alerts and blocking the traffic automatically. As an example:

a. Calling Number blocks

System is able to set the thresholds that will trigger the alarms and automatic blockage of the specified traffic when the system finds patterns that may indicate suspicious activity in calling numbers.



- b. Called Number blocks
System is able to set the thresholds that will trigger the alarms and automatic blockage of the specified traffic when the system finds patterns that may indicate suspicious activity in called numbers.
- c. Carrier blocks
System is able to set the thresholds that will trigger the alarms and automatic blockage of the specified traffic when the system finds patterns that may indicate suspicious activity from a specific Carrier.
- d. Anonymous blocks
System is able to set the thresholds that will trigger the alarms and automatic blockage of the specified traffic when the system finds patterns that may indicate suspicious activity from an unknown ANI.
- e. Wangiri blocks
System is able to set the thresholds by number or destination that will trigger the alarms and automatic blockage of the specified traffic when the system finds patterns that may indicate suspicious Wangiri traffic.
- f. RMD Database flag
This system flag blocks calls with both origination and destination numbers in the USA except for some defined carriers (only carriers included in the RMD Database have this flag active)

3. Traceback

We commit to respond in a timely manner to all traceback requests from the Commission, Law Enforcement Agencies and the industry Traceback Consortium and cooperate with such entities to stop any illegal robocaller that tries to use our network.

Yours sincerely,

Orange España Comunicaciones Fijas S.L.U.