

Robocall Mitigation Plan

Orange Business Services US, Inc. ("Orange Business")

A. Company Information

(1) Call Chain Role

Orange Business is a voice service provider which originates and terminates traffic to its customers. Orange Business mainly provides Voice over Internet Protocol ("VoIP") services to enterprise customers. Orange Business provides services to its enterprise customers in conjunction with its affiliate France Telecom Corporate Solutions, L.L.C.

(2) Information regarding principals, affiliates, subsidiaries, and parent company (US affiliates that provide telecommunications identified herein)

Orange SA
111 quai du president Roosevelt,
CS 70222
92449 Issy-Les-Moulineaux CEDEX, France

France Telecom Corporate Solutions, L.L.C.
11921 Freedom Drive
Suite 720
Reston, VA 20190

France Telecom Long Distance USA, LLC dba Orange Carriers USA
11921 Freedom Drive
Suite 720
Reston, VA 20190

(3) Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling

None.

(4) Operating Company Number (OCN) if any.

None.

B. Mitigation Plan

(1) Orange Business meets its existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls.

Orange Business customers are global enterprises that take security issues very seriously and implement robust Information Technology (“IT”) and Security measures to protect their equipment and infrastructure. In case of a fraud incident occurring at a customer site, Orange Business relies on customer intervention to address the root cause of the security breach. Orange Business, working with its affiliate France Telecom Corporate Solutions, L.L.C., also employs a fraud detection team that works proactively to detect any potential fraud that has penetrated its network. Orange Business has processes in place to monitor traffic to receive alerts in case of non-standard or abnormal traffic patterns. This includes monitoring “call attempts per second” (a measure of the total number of call requests made by a telecommunications system or network each second) to help identify any traffic anomalies. In addition, to avoid/reject robocalls or large, unexpected marketing campaigns, Orange Business has defined a default parameter for its customers. If a traffic pattern anomaly is identified, the customer is contacted and asked to confirm whether the traffic is legitimate or not. In case the traffic is deemed illegitimate, the customer has the first responsibility to block it, with the goal of stopping fraudulent activity at its origin. If the customer needs assistance, then Orange Business proceeds to block the traffic. In the rare circumstance where Orange Business identifies suspicious traffic and confirms it is illegal, the policy is to block the illegal traffic.

a. Fraud detection process consists of the following main phases:

1. Detection: Using dedicated fraud detection systems deployed at different parts of the network.
2. Analysis / qualification: Specialists review data to judge likelihood of fraud and appropriate actions to be taken.
3. Notification: Typically accomplished via customer service manager or account team to agreed customer contact.
4. Act on Countermeasures: Blocking strategy agreed with customer and implemented by Orange Business and its partner affiliates.
5. Customer Investigation / Resolution: Customer closes root cause security issue.
6. Follow-up: Ensure monitoring and reporting in case of further fraud breaches.

(2) “Know-your-customer” initiatives

Orange Business employs a variety of “know-your-customer” initiatives to help mitigate the risk that its customers would attempt to use the network to initiate an illegal robocalling campaign. Orange Business serves primarily global enterprise customers and has a rigorous process of vetting its customers, including, but not limited to, checking its customers legal identity, credit and financial worthiness, and thereafter requiring them to maintain appropriate prevention, detection and remedial measures to ensure they are not subject to Economic Sanctions. Orange Business customers are Tier 1 customers with

qualified IT and security personnel and security systems that are nearly impossible to breach due to firewalls and other security measures.

(3) “Know-your-upstream provider” procedures in place designed to mitigate illegal robocalls

Orange Business employs a rigorous due diligence process when selecting a carrier as an upstream provider. As a general rule, we partner primarily with Tier 1 carriers with a demonstrated reputation for high quality IT and Security departments. We expect their security personnel are qualified and that they have a robust fraud detection and prevention program. Upstream providers are registered in the Robocall Mitigation Database, comply with relevant regulations and have a robocall mitigation plan in place.

(4) Call analytics systems used to identify and block illegal traffic

As indicated above, we employ a fraud detection process that relies on tools that have been developed internally. While we may use some third-party software in our tools, they have been customized to meet our own requirements. We use the “call attempt per second” analysis, among other tools, to detect anomalies and to identify and ultimately block or secure the blocking of illegal traffic.

(5) Contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls

a. End-User Provisions

Agreements with end-user enterprise customers using our outbound voice service includes general language that is designed to prevent any unlawful or fraudulent use of our services, including the initiation of illegal robocalls. All customers must comply with our Fair Use Policy which expressly prohibits unlawful robocalling. Additionally, our Fair Use Policy states that the service is exclusively intended for standard business use and calling, and the customer agrees that users will not use our service for: (a) call center or mass marketing inbound calls, (b) voting line, (c) continuous and extensive call forwarding, (d) fax broadcast or fax "blasting", (e) reselling subscription and minutes, (f) sharing subscriptions between users, (g) inbound audioconferencing services, and (h) calling inconsistent with normal, individual subscription use. Caller ID manipulation or spoofing in violation of applicable law, rule, or regulation is strictly forbidden, and Orange Business supports industry standard Caller ID presentation and restrictions. Orange Business also may restrict or prohibit the use of certain Caller ID in accordance with applicable law or regulation, and Orange Business may stop all voice traffic (whether incoming or outgoing) associated with any Caller ID that is restricted or prohibited by the relevant regulatory or governmental authority(ies). Where a customer is found to be in violation of our Fair Use Policy, Orange Business may immediately suspend or terminate services to the customer.

b. Upstream Provider Provisions

Contractual provisions with upstream providers prohibit sending of illegal robocalls. If we find that an upstream provider is sending suspicious robocalls, we warn them to stop. If such traffic continues, it is our policy to invoke our rights under our agreements with upstream providers to terminate service due to fraud.

(6) Traceback

Orange Business commits to respond to traceback requests from the Federal Communications Commission, law enforcement and the registered traceback consortium. Orange Business commits to cooperate fully in investigating and stopping illegal robocallers that use our service to originate, carry, or process illegal robocalls.