

**Robocall Mitigation Plan
Of
France Telecom Corporate Solutions, L.L.C. ("FTCS")**

A. Company Information

(1) Call Chain Role

FTCS is a voice service provider which originates and terminates traffic to its customers. FTCS mainly provides VoIP services to enterprise customers. FTCS provides services to its enterprise customers in conjunction with its affiliate Orange Business Services U.S. Inc.

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

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

Orange Business Services U.S. Inc. ("Orange Business")(U.S. affiliate)
11921 Freedom Drive
Suite 720
Reston, VA 20190

France Telecom Long Distance USA, LLC dba Orange Carriers USA (U.S. affiliate)
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.

FTCS' OCN – 766C

B. Mitigation Plan

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

Our customers are global enterprises who take the issue of security very seriously and implement robust IT and Security measures to protect their equipment and infrastructure. In case of a fraud incident occurring at a customer site, FTCS relies on customer intervention to address the root cause of the security breach. FTCS, working with its affiliate Orange Business, also employs a fraud detection team that works proactively to detect any potential fraud that has penetrated our network. FTCS has processes in place where it is constantly monitoring traffic to receive alerts in case of non-standard or abnormal traffic patterns. This includes monitoring of Call Attempts Per Second (“CAPS”) to identify any traffic anomalies. CAPS is a measure of the total number of call requests that can be made by a telecoms system or network each second. In addition, to avoid/reject Robocalls or Large unexpected marketing campaigns, FTCS has defined a default parameter for all of our customers. If a traffic pattern anomaly is identified, the customer is contacted immediately and asked to confirm whether the traffic is legitimate or not. In case the traffic is deemed illegitimate, it is the customer who has the first responsibility to block it. This is in keeping with the goal of stopping the fraudulent activity at its origin. If the customer needs our assistance, then FTCS proceeds to block the traffic. In the rare circumstance where FTCS identifies suspicious traffic and is able to confirm with certainty that it is illegal, then our policy is to block this illegal traffic immediately.

- a. Our 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 likeliness of fraud and appropriate actions
 3. Notification: Usually done via customer service manager or account team to agreed customer contact
 4. Act on Countermeasures: Blocking strategy agreed with customer and implemented by FTCS 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

FTCS employs a variety of “know-your-customer” initiatives to help mitigate the risk that its customers would attempt to use Orange’s network to initiate an illegal robocalling campaign. FTCS 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. FTCS 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

FTCS 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 that 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) describes any call analytics systems it uses 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 amongst others tools to detect anomalies and to identify and ultimately block or secure the blocking of illegal traffic.

- (5) Description of contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls.

a. End-User Provisions

Our Customer Contract 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 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. CLI/ANI manipulation or spoofing in violation of applicable law, rule, or regulation is strictly forbidden, and FTCS supports industry standard CLI presentation and restrictions. FTCS also may restrict or prohibit the use of certain CLI/ANI in accordance with applicable law or regulation, and FTCS may stop all voice traffic (whether incoming or outgoing) associated with any CLI/ANI 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, FTCS 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 us 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

FTCS commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. FTCS commits to cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.