

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Robocall Mitigation Plan

)
)
)
)
)

WC Docket No. 17-97

CERTIFICATION PURSUANT TO 47 C.F.R. 64.6305(d)

1. I, Jesus Pena, EVP and CXO, United Data Technologies, Inc. ("UDT"), submits this certification to the extent UDT operates as a voice service provider.
2. UDT has implemented the STIR/SHAKEN authentication framework across its network as described in its Robocall Mitigation Database ("RMD") registration. All calls originated on the UDT network are subject to the attached Robocall Mitigation Program described in Appendix A. No prior UDT certification has been removed by FCC action and UDT has not been prohibited from filing in the RMD.
3. At no time in the prior two years has UDT (and/or any entity for which the filing entity shares common ownership, management, directors, or control) been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description.
4. The statements and information contained in this certification are accurate and complete to the best of my knowledge and belief.
5. Pursuant to 47 C.F.R. § 1.16, I certify under penalty of perjury that the foregoing is true and correct.

Name: Jesus Pena

Title: EVP and CXO

Signature: Jesus Pena
Jesus Pena (Jan 21, 2025 10:56 EST)

Date: 01/21/25

APPENDIX A

UNITED DATA TECHNOLOGIES, INC. STATEMENT IN SUPPORT OF ITS VOICE SERVICE PROVIDER CERTIFICATION AND DESCRIPTION OF ITS ROBOCALL MITIGATION PROGRAM

United Data Technologies, Inc. ("UDT"), a voice service provider directly serving end users certifies that it has fully implemented STIR/SHAKEN as indicated in its Robocall Mitigation Database registration.

This Robocall Mitigation Plan describes the specific measures that UDT has implemented as of January 1, 2025. UDT continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.

Business name and address: United Data Technologies, Inc., 2900 Monarch Lakes Blvd., Suite 300, Miramar, FL 33027

OCN: 058L

Contacts: Kathryn O'Connor, Chief of Staff and Senior Counsel, Legal and Compliance Department, United Data Technologies, Inc., 2900 Monarch Lakes Blvd., Suite 300, Miramar, FL 33027, legalsupport@udtonline.com, 954-308-5256, as well as Mr. Dana Briggs, Senior Director of Service Excellence, dbriggs@udtonline.com

Specific reasonable steps UDT has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program:

UDT has implemented "know your customer" and traffic monitoring processes to mitigate the risk that it may inadvertently process or route illegal robocalls on behalf of its customers. UDT follows procedures for ensuring it knows the identities of its customers, especially ones whose service permits them to engage in high volume calling campaigns, such as businesses engaged in telemarketing or contacting their customers for legitimate purposes. UDT has a customer onboarding process designed to proactively identify and prevent those that may engage in illegal robocalling from becoming UDT customers. All UDT customers must provide their names, addresses, verified e-mail address(es), verified phone number(s), validated payment information, and, if the customer is a legal entity, the state or country of formation, contact person, and company registration number.

UDT verifies the information obtained from the customer through the collection and validation of the following documentation:

1. **Proof of Identity:** A digital copy of a current valid government issued form of identification for the applicant, such as a passport or driver's license.
2. **Proof of Business Legal Entity:** If a business, official documentation verifying existence of the legal entity and registered address, which may be a copy of one of the following: business license, registry of a non-profit organization, notarized business lease, articles of incorporation, company tax number/ID/EIN or other documentation appropriate to the customer's country of operations. SEC filers may supply their CIK code, which may be verified via the SEC website.
3. **Proof of Authorized Individual:** If a business, official documentation verifying that the individual purporting to act on behalf of the business has the authority to do so. This proof may include a copy of a letter of authority, board minutes or other suitable documentation, or public registration information.

To the extent that UDT receives information from law enforcement or other sources that a customer is engaged in illegal calling, our policy is to cooperate fully, including by providing the identity of any suspected illegal robocaller pursuant to legal service of process. UDT's contracts include clauses granting it the right to suspend or terminate service if customers are making illegal calls or otherwise violating UDT's acceptable use provisions. Customers may also be liable for any financial penalties imposed on UDT for fraudulent traffic sent from the customer.

UDT has personnel that will monitor, detect and analyze the use of UDT services and traffic patterns on its network that can help identify potentially illegal robocalls, such as: (1) Short duration calls less than 6 seconds long; (2) Multiple calls per minute from the same customer; (3) Low call answer rates for calls from a particular customer; (4) Calls to high fraud destinations; (5) Dialing patterns; (6) Calls to numbers on Do-Not-Call lists; (7) Traceback requests; and (8) Unusual changes in a customer's established traffic patterns.

UDT will also rely on its network service provider partners to identify and block invalid, unallocated or otherwise obviously illegal telephone numbers. UDT utilizes third party analytics providers to identify and block illegal traffic. The name of the third party analytics providers are Sansay NSS and/or TransNexus ClearIP.

Upstream Providers: UDT's contracts with upstream providers require that the provider comply with all relevant laws, including in many instances specific provisions prohibiting the transmission of fraudulent traffic and robocalls. UDT's contracts also permit it to terminate the upstream provider's right to send traffic to UDT if any contractual provision is violated.

Commitment to Respond to Traceback Requests: UDT commits to respond fully and within twenty-four (24) hours to traceback requests from law enforcement, the Federal Communications Commission, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocalls that use its services to originate such calls.

Robocall Mitigation Database Filings: UDT checks the Robocall Mitigation Database and only accepts calls from providers if those providers' filings appear in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action.

Affiliated entities covered by UDT's Robocall Mitigation Plan: NONE