JOSHUA H. STEIN
ATTORNEY GENERAL

TRACY NAYER
SPECIAL DEPUTY ATTORNEY GENERAL

October 18, 2024

Andrés Sánchez, CEO
Gabriel Sánchez, Executive Chairman
Santiago Sánchez, VP of Operations
iDentidad Advertising Development, LLC, dba iDentidad Telecom
848 Brickell Avenue, Suite 810
Miami, FL 33131
Sent via certified mail, return receipt requested, and via email to ssanchez@identidadtech.com; noc@identidadtelecom.net; admin@identidadtelecom.net

Re: NOTICE from the Anti-Robocall Multistate Litigation Task Force Concerning iDentidad Advertising Development LLC's Involvement in Suspected Illegal Robocall Traffic

Dear Mssrs. Sánchez:

The Anti-Robocall Multistate Litigation Task Force ("Task Force")[1] has been made aware that iDentidad Advertising Development LLC dba iDentidad Telecom ("iDentidad") is transmitting suspected illegal robocall traffic on behalf of one or more of its customers. This Notice is intended to inform iDentidad about the Task Force's concerns regarding its call traffic, and to caution iDentidad that it should cease transmitting any illegal traffic immediately.

As iDentidad well knows, originating and transmitting illegal robocalls are violations of the Telemarketing Sales Rule,[2] the Telephone Consumer Protection Act,[3] and/or the Truth in Caller ID Act,[4] as well as state consumer protection statutes. On November 27, 2023, iDentidad was

[1] The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall ecosystem that are identified as being responsible for significant volumes of illegal and fraudulent robocall traffic routed into and across the country.

[2] 15 U.S.C. §§ 6101–6108; 16 C.F.R. §§ 310.3, 310.4.

[3] 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

[4] 47 U.S.C. § 227(e); 47 C.F.R. § 64.1604.

issued a Cease-and-Desist Demand[5] from the Federal Trade Commission ("FTC"), and a Notice of Important Gateway Provider Obligations[6] from the Federal Communications Commission ("FCC"). The FTC's Cease-and-Desist provided that iDentidad was knowingly routing and transmitting illegal robocall traffic identified therein between August 21, 2022, and October 3, 2023.[7] The FCC's Obligations Notice provided that, in its role as a gateway provider, iDentidad received a significant volume of traceback requests concerning apparently illegal traffic iDentidad transmitted on behalf of overseas providers.[8] Both the FTC's Cease-and-Desist and the FCC's Obligations Notice referenced applicable federal laws and rules, and iDentidad's legal obligations under the same.

With this Notice, the Task Force requests that iDentidad take steps to prevent its network from continuing to be a source of suspected illegal robocalls. If, after receiving this Notice, iDentidad transmits—or continues to transmit—calls that are associated with illegal robocall campaigns, the Task Force may pursue an enforcement action against iDentidad and its principal owners and/or operators.

Task Force's Concerns about iDentidad's Call Traffic

As part of its investigation into the transmission of illegal robocalls and the providers and entities who originate and/or route them, the Task Force regularly reviews call traffic information provided by several industry sources, including USTelecom's Industry Traceback Group ("ITG")[9] and ZipDX LLC ("ZipDX")[10]. Based on information available to the Task Force, it appears that

---

[5] FTC, *Cease and Desist Demand to iDentidad Advertising Development, LLC*, https://www.ftc.gov/system/files/ftc_gov/pdf/pointofnoentry-identidadcease-desistletter.pdf (hereinafter "FTC's Cease-and-Desist").

[6] FCC, *Notice of Important Gateway Provider Obligations to iDentidad Advertising Development, LLC*, https://docs.fcc.gov/public/attachments/DOC-398676A1.pdf (hereinafter "FCC's Obligations Notice").

[7] FTC's Cease-and-Desist at 1–2.

[8] FCC's Obligations Notice at 1.

[9] Established in 2015, the ITG is a private collaborative industry group—composed of providers across wireline, wireless, VOIP, and cable services—that traces and identifies the sources of suspected illegal and suspicious robocalls. In December 2019, Congress enacted the Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ("TRACED Act") to combat the scourge of unlawful robocalls. *See* Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019). Following its enactment, the Federal Communications Commission designated the ITG as the official private-led traceback consortium charged with leading the voice communications industry's efforts to trace the origin of suspected illegal robocalls through various communications networks through tracebacks. *See* 47 C.F.R. § 64.1203.

[10] ZipDX is a provider of web- and phone-based collaboration services, which also focuses resources on developing and making technology available that is directed at mitigating illegal robocalls and other telephone-based fraud and abuse. ZipDX's proprietary tool "RRAPTOR" is

iDentidad is transmitting calls associated with high-volume illegal and/or suspicious robocall campaigns.

Call traffic data from the ITG shows that it issued at least **190 traceback notices** to iDentidad since 2021—and as recently as last week—for calls it originated, accepted, and/or transmitted onto and across the U.S. telephone network. More than 60 of these traceback notices have been issued to iDentidad *after* it was issued the FTC's Cease-and-Desist and the FCC's Obligations Notice. The traceback notices from the ITG—some of which were also referenced in the FTC's Cease-and-Desist—cited recurrent high-volume illegal and/or suspicious robocalling campaigns concerning, in part, IRS/SSA government imposters, tax relief, financial impersonation, private entity imposters, Chinese-language delivery and impersonations, and utilities disconnect scams, with iDentidad serving as the gateway provider[11] for almost 90% of this call traffic.

With respect to these scams, in at least two instances in the last month or so, non-residents of Illinois contacted the Office of the Illinois Attorney General to report receiving calls that appeared, based on caller ID, to have originated from a toll-free hotline used by the Office of the Illinois Attorney General. The Office of the Illinois Attorney General had not attempted to contact these people, and it is believed the calls were part of a campaign of suspicious robocalls.

Further, ITG traceback data shows that iDentidad reported receiving illegal and/or suspicious robocalls directly from foreign service providers not listed in the FCC's Robocall Mitigation Database ("RMD") at the time of the calls. Since April 2023, ITG data shows that iDentidad has reported that at least 37 traced calls were received from foreign providers not listed in the RMD. iDentidad's upstream providers not listed in the RMD at the time of the calls include Orange Romania, Telin Neutrafix, TVoice PTE. LTD, Sipstatus Global Ltd., Blue Cloud Telecom PTE LTD, and Quick Telecom Limited. Providers may only accept calls directly from foreign providers using U.S. telephone numbers in the caller ID field when that foreign provider is listed in the RMD.[12] The Task Force urges iDentidad to review its obligations under the rules and to immediately cease accepting calls directly from providers not listed in the RMD.

---

one such technology, which is an automated robocall surveillance tool that captures call recordings and information for calls largely associated with high-volume suspicious calling campaigns, and identifies the providers who have affixed their SHAKEN signatures to each of the captured calls, indicating that the provider is in the call path and whether those providers have attested to knowing the calling party who made the suspicious call and/or knowing of the calling party's right to use that calling number to make that suspicious call. *See* ZipDX, What is RRAPTOR?, https://legalcallsonly.org/what-is-rraptor/ (last visited Oct. 17, 2024).

[11] *Advanced Methods to Target and Eliminate Unlawful Robocalls,* CG Docket No. 17-59; *Call Authentication Trust Anchor*, WC Docket No. 17-97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking, 87 FR 42916, 42917–18, para. 7 (2022) (defining a "gateway provider" as "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider").

[12] *See* 47 C.F.R. § 64.6305(g).

Information available from ZipDX also indicates that iDentidad attested to calls for a number of the same high-volume robocalling campaigns for which it received and/or continues to receive traceback notices from the ITG. For instance, in just the 12 months, ZipDX identified **497 suspicious calls** transmitted by iDentidad from 452 unique calling numbers,[13] many of which exhibit characteristics indicative of calls that are violations of federal and state laws; over 470 of these calls were made to numbers that have been registered on the National Do Not Call Registry.[14] Given the prolific nature of the calls, the Task Force is concerned about whether iDentidad is taking any proactive steps to mitigate this traffic.

Further, 100% of these calls were signed by iDentidad with a "C"-level STIR/SHAKEN attestation. However, as noted above, information available to the Task Force indicates that iDentidad often, if not exclusively, serves as the originating or gateway provider in the call path, which would require iDentidad to label calls with an "A"- or "B"-level attestation consistent with its relationship to the customers and its KYC policies. In such cases, labeling calls with a "C"-level attestation when iDentidad is the gateway provider or the originating service provider is improper.[15]

Thus, the information available to the Task Force shows that iDentidad is involved in, at a minimum, transmitting call traffic indicative of, and associated with, recurrent high-volume illegal and/or suspicious robocalling campaigns and/or practices, which conduct could subject iDentidad to damages, civil penalties, injunctions, and other available relief provided to State Attorneys General under both federal and state laws.

Overview of Select Relevant Laws

Telemarketing Sales Rule (15 U.S.C. §§ 6101–6108; 16 C.F.R. Part 310)

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act which directed the FTC to prescribe rules prohibiting deceptive telemarketing acts or practices.[16] Pursuant to this directive, the FTC promulgated the Telemarketing Sales Rule

[13] The use of many unique calling numbers for this volume of called numbers indicates a suspicious pattern in your call traffic of "snowshoeing" or "snowshoe spoofing," which is a practice often employed by illegal robocallers and telemarketers to circumvent the protections of the STIR/SHAKEN call authentication framework by using significant quantities of unique numbers for caller IDs on a short-term or rotating basis in order to evade behavioral analytics detection, or to bypass or hinder call blocking or call labeling analytics based on the origination numbers. Telephone numbers used for snowshoeing sometimes cannot themselves receive incoming calls, which has the effect of impeding an audit of the legitimacy of these calling numbers.

[14] Most calls captured by RRAPTOR are calls made to phone numbers that have been registered on the National Do Not Call Registry.

[15] *See* Secure Telephone Identity Governance Authority, *Improper Authentication and Attestation*, https://sti-ga.atis.org/wp-content/uploads/2023/07/230724-Improper-Auth-and-Attest-Def-Final.pdf.

[16] 15 U.S.C. § 6102.

("TSR"). It is a violation of the TSR for voice service providers to provide substantial assistance to customers that the provider "knows or consciously avoids knowing" are engaged in practices that violate TSR provisions against deceptive and abusive telemarketing acts or practices.[17] State Attorneys General have concurrent authority with the FTC to sue to obtain damages, restitution, or other compensation on behalf of their citizens for violations of the TSR.[18]

Telephone Consumer Protection Act (47 U.S.C. § 227; 47 C.F.R. §§ 64.1200 and 64.1604)

Under the Telephone Consumer Protection Act ("TCPA"), the FCC promulgated rules restricting calls made with automated telephone dialing systems and calls delivering artificial or prerecorded voice messages.[19] Additionally, the TCPA generally prohibits solicitation calls placed to numbers on the National Do Not Call Registry.[20] State Attorneys General are authorized to bring enforcement actions to enjoin violative calls and recover substantial civil penalties for *each violation* of the TCPA.[21] The TCPA exempts from its prohibitions calls made for emergency purposes and certain other calls,[22] including those made with the "prior express consent" of the called party or with "prior express *written* consent" of the called party for telemarketing calls.[23] Note, however, single consents purportedly given by a consumer to large groups of marketers listed on an alternate webpage are insufficient to satisfy this exemption.[24]

---

[17] 16 C.F.R. § 310.3(b).

[18] 15 U.S.C. § 6103; 16 C.F.R. § 310.7.

[19] 47 U.S.C. § 227(b)(1)(A)(iii), (b)(1)(B); 47 C.F.R. § 64.1200(a)(1)–(3).

[20] 47 U.S.C. § 227(c); 47 C.F.R. § 64.1200(c)(2).

[21] 47 U.S.C. § 227(g)(1).

[22] 47 U.S.C. § 227(b)(1)(A)–(B), (b)(2)(B); 47 C.F.R. § 64.1200(a)(1)–(3), (a)(9).

[23] 47 U.S.C. § 227(b)(1)(A)–(B); 47 C.F.R. § 64.1200(a)(1)–(3), (f)(9).

[24] For example, in November 2022, the FCC issued an order requiring all voice service providers to block calls from provider Urth Access, LLC. In response to allegations concerning the transmission of illegal robocalls, Urth Access claimed to have obtained express consent for each of the calls. However, that consent stemmed from websites where consumers purportedly agreed to receive robocalls from over 5,000 "marketing partners" listed on a separate site. The FCC found this type of agreement insufficient to constitute express consent. *See FCC Orders Voice Service Providers to Block Student Loan Robocalls*, https://www.fcc.gov/document/fcc-orders-voice-service-providers-block-student-loan-robocalls (Order); *FCC Issues Robocall Cease-and-Desist Letter to Urth Access*, https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letter-urth-access (Cease-and-Desist Letter). Additionally, in March 2023, the FCC issued a Notice of Proposed Rulemaking expressing its intent to expressly ban the practice of obtaining a single consumer consent as grounds for delivering calls and text messages from multiple marketers on subjects beyond the scope of the original consent. *See Targeting and Eliminating Unlawful Text Messages*, CG Docket No. 21-402, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2744, 2765–66 (Mar. 17, 2023), https://www.fcc.gov/document/fcc-

Truth in Caller ID Act (47 U.S.C. § 227(e))

Under the federal Truth in Caller ID Act, it is generally unlawful for a person to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."[25] State Attorneys General have the authority to bring enforcement actions for violations of the Truth in Caller ID Act and its prohibition against illegal caller identification spoofing.[26] Such violative conduct can lead to assessments of civil penalties of up to $10,000 for each violation, or three times that amount for each day of continuing violations.[27] Note that any penalties for violations of the Truth in Caller ID Act are in addition to those assessed for any other penalties provided for by the TCPA.[28]

General Note regarding State Laws

In addition to their authority to enforce the above federal statutes, State Attorneys General are empowered to enforce their respective state laws regulating various aspects of the initiation and transmission of illegal robocall and telemarketing call traffic across the U.S. telephone network. Voice service providers transmitting calls into and throughout the states are obligated to familiarize themselves with, and abide by, all applicable state laws.

Requested Action in Response to this Notice

The Task Force requests that you review this Notice in detail and carefully scrutinize and actively investigate any suspected illegal call traffic that is, and has been, accepted and transmitted by and through iDentidad's network, in order to ensure that your business is following all applicable federal and state laws and regulations, including those referenced above. If further investigation shows that you continue to assist your customers by initiating and/or transmitting call traffic not dissimilar from the traffic highlighted in this Notice, the Task Force may decide to pursue an enforcement action against you and your principal owners and operators. For your information, we have informed several of our federal law enforcement counterparts, including our colleagues at the FCC's Enforcement Bureau, of the Task Force's intention to issue this Notice to iDentidad. Finally, this Notice *does not* waive or otherwise preclude the Task Force from bringing

---

adopts-its-first-rules-focused-scam-texting-0. We note also that this interpretation is consistent with the FTC's interpretation of the express consent requirement of the TSR. *See* Federal Register, Vol. 73 No. 169, 2008 at 51182, https://www.govinfo.gov/content/pkg/FR-2008-08-29/pdf/E8-20253.pdf (Consumer's agreement with a seller to receive calls delivering prerecorded messages is nontransferable); *FTC, Complying with the Telemarketing Sales Rule, The Written Agreement Requirement*, https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement.

[25] 47 U.S.C. § 227(e)(1); 47 C.F.R. § 64.1604.

[26] 47 U.S.C. § 227(e)(6).

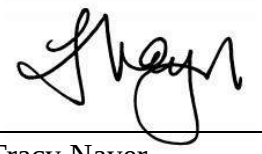
[27] 47 U.S.C. § 227(e)(5)(A), (e)(6)(A).

[28] *Id.*

an enforcement action related to conduct preceding the date of this Notice, including conduct that resulted in violations related to the call traffic referenced in this Notice.

The Task Force remains steadfast in its resolve to meaningfully curb illegal robocall traffic. Please direct any inquiries regarding this Notice to my attention at tnayer@ncdoj.gov. Your anticipated cooperation is greatly appreciated.

Sincerely,



Tracy Nayer
Special Deputy Attorney General
Consumer Protection Division
North Carolina Department of Justice