



Federal Communications Commission
Enforcement Bureau
45 L Street, NE
Washington, DC 20554

July 7, 2022

VIA ELECTRONIC DELIVERY AND CERTIFIED MAIL - RETURN RECEIPT REQUESTED

To: Dave Dimnick
CEO
SipKonnnect LLC
7901 4th St. N
Suite 5907
St. Petersburg, FL 33702
support@sipkonnnect.com

Re: Official Correspondence from the Federal Communications Commission

Dear Mr. Dimnick:

We have determined that SipKonnnect LLC (“SipKonnnect”) is apparently originating illegal robocall traffic on behalf of one or more of its clients. You should investigate and, if necessary, cease transmitting such traffic immediately and take steps to prevent your network from continuing to be a source of apparent illegal robocalls. As noted below, downstream voice service providers will be authorized **to block all of SipKonnnect’s traffic** if you do not (1) take steps to “effectively mitigate illegal traffic within 48 hours,” and (2) inform the Commission and the Traceback Consortium within fourteen (14) days of the date of this letter (Thursday, July 21, 2022) of the steps you have taken to “implement effective measures” to prevent customers from using your network to make illegal calls.¹ Additionally, if you continue knowingly or negligently to originate illegal robocall campaigns after responding to this letter, **we may remove your certification from the Robocall Mitigation Database thereby requiring all intermediate providers and terminating voice service providers to cease accepting your traffic.**²

Basis for finding apparent violations. You are receiving this letter because our investigation revealed that SipKonnnect apparently originated multiple illegal robocall campaigns, as set forth in Attachment A. These robocalls are connected with a robocalling enterprise led by Roy Cox, Jr., Aaron Michael Jones, their individual associates, and associated entities (collectively, the Cox/Jones/Sumco Panama Operation).³ The Federal Communications Commission’s Enforcement Bureau (Bureau) works

¹ See 47 CFR § 64.1200(k)(4).

² *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1903, para. 83 & 1904, para. 86 (2020); 47 CFR § 64.6305.

³ The Cox/Jones/Sumco Panama Operation includes the following individuals: Roy Melvin Cox Jr., resident of Tustin, California; Aaron Michael Jones, resident of Orange County, California; Scott Presta, resident of Lakeway, Texas; Kathleen Presta, resident of Lakeway, Texas; Stacey Yim, resident of La Crescenta, California; Jovita Migdaris Cedeno Luna, resident of San Francisco, Panama; Livia Szuromi, resident of Budapest, Hungary; Maria Alejandra Gonzalez; Davinder Singh; Andrea Baloghne Horvath, resident of Budapest, Hungary; Adam Radimiri; June Batista, resident of Costa Mesa, California; and Julie K. Bridge, resident of Upland, California. The

closely with the USTelecom’s Industry Traceback Group (Traceback Consortium), which is the registered industry consortium selected pursuant to the TRACED Act to conduct tracebacks.⁴ Between January 15th and June 15th, 2022 the Traceback Consortium investigated prerecorded voice message calls that customers of YouMail had flagged as illegal robocalls made without consent.⁵ The calls are prerecorded advertising solicitations that apparently were made without consent of the called parties and absent an emergency purpose, in violation of section 227(b) of the Telephone Consumer Protection Act.⁶ The calls apparently were made with the intent to violate the Telephone Consumer Protection Act of 1991, in violation of the TRACED Act,⁷ and the calls displayed inaccurate or misleading caller identification, with an apparent intent to defraud, cause harm, or wrongfully obtain something of value, in violation of the Truth in Caller ID Act.⁸ Moreover, one of the individuals involved, Roy Cox, entered into a settlement with the Department of Justice and the Federal Trade Commission in which he accepted a permanent ban on all telemarketing activities.⁹ Call detail records obtained by the Bureau via the Traceback Consortium indicate that the calls either directly originated from, or were carried by, each of the Originating Providers.¹⁰

The Traceback Consortium conducted tracebacks and determined that SipKconnect originated the calls. The Traceback Consortium previously notified you of these calls and provided you access to supporting data identifying each call, as indicated in Attachment A. Further, the numerous tracebacks to SipKconnect as an originator indicate that you are apparently knowingly or negligently originating illegal robocall traffic. Under our rules (and as explained further below), providers that originate illegal robocall traffic face serious consequences, including blocking by downstream providers of all of the originating provider’s traffic. To avoid such blocking, you must take corrective actions immediately.

Actions You Should Take Now. SipKconnect should take the following steps to resolve this matter:

1. Promptly investigate the transmissions identified in Attachment A.
2. If necessary, “effectively mitigate” the identified unlawful traffic by determining the source of the traffic and preventing that source from continuing to originate such traffic.
3. Implement effective safeguards to prevent customers from using your network as a platform to originate illegal calls.
4. Within 48 hours, inform the Commission and the Traceback Consortium of steps taken to mitigate the identified apparent illegal traffic. If you have evidence that the

Cox/Jones/Sumco Panama Operation also includes the following entities: Sumco Panama S.A.; Sumco Panama Inc.; Tech Direct LLC; Posting Express Inc.; 7 Sundays Inc.; and Texas Outdoor Adventures Inc.

⁴ *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, DA 21-1047 (EB 2021) (*2021 Consortium Selection Order*). See also Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274, Sec. 13(d) (2019) (TRACED Act).

⁵ See 47 U.S.C. § 227(b); 47 CFR § 64.1200(a).

⁶ Telephone Consumer Protection Act of 1991, 1991 Enacted S. 1462, 102 Enacted S. 1462, 105 Stat. 2394; 47 U.S.C. § 227.

⁷ Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, § 3, Pub. L. No. 116-105, 133 Stat. 3274 (2019) (codified as amended in 47 U.S.C. § 227).

⁸ Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

⁹ *U.S. v. Roy M. Cox, Jr. et al*, No. 8:11-cv-01910-DOC-JPR (C.D. Cal. 2013).

¹⁰ See call detail record information on file in FCC File No. EB-21-00031913.

transmissions identified in Attachment A were legal calls, present that evidence to the Commission and the Traceback Consortium.

5. Within fourteen (14) days of the date of this letter (Thursday, July 21, 2022) inform the Commission and the Traceback Consortium of the steps SipKconnect is taking to prevent customers from using its network to transmit illegal robocalls (i.e. robocall mitigation measures).¹¹ Failure to provide this information within 14 days shall be equivalent to having failed to put effective measures in place.¹²

Consequences for Failure to Comply. If after 48 hours of issuance of this letter SipKconnect continues to route or transmit harmful robocall traffic from the entities involved in these campaigns, downstream U.S.-based voice service providers may begin blocking all calls from SipKconnect notifying the Commission of their decision and providing a brief summary of their basis for making such a determination.¹³ If SipKconnect fails to take sufficient mitigating actions to prevent new and renewing customers from using its network to originate illegal robocalls, then downstream U.S.-based providers may block calls following notice to the Commission. **Failure to act within the deadlines authorizes U.S.-based voice service providers to block ALL call traffic transmitting from your network, permanently.**

Furthermore, if you fail to take the actions listed above, or knowingly or negligently continue to originate unlawful robocall campaigns after responding to this letter, we may find that your certification in the Robocall Mitigation Database is deficient and direct the removal of your certification from the database.¹⁴ Removal of a certification from the Robocall Mitigation Database requires all intermediate providers and terminating voice service providers to immediately cease accepting all of your calls.¹⁵

¹¹ See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7630, para. 43 (2020) (*Call Blocking Safe Harbor Report and Order*).

¹² You are encouraged to reach out to the Commission before the deadline if you anticipate needing more time to execute this step.

¹³ In July 2020, the Commission adopted the *Call Blocking Safe Harbor Report and Order*, which authorized voice service providers to block illegal robocalls. *Call Blocking Safe Harbor Report and Order*, 35 FCC Rcd at 7628, para. 37; see also 47 CFR § 64.1200(k)(3)-(4). If the Commission identifies illegal traffic, based on information obtained through traceback such as that provided by the Traceback Consortium, the Commission may notify the voice service provider that it is transmitting identified probable illegal calls (or “bad traffic”) and, upon receipt of notification, the voice service provider should investigate promptly and take any steps that may be necessary to prevent the illegal caller from continuing to use the network to make such calls. Furthermore, if the notified voice service provider fails to take effective mitigation measures within 48 hours, any downstream voice service provider may block the calls from the notified provider. *Call Blocking Safe Harbor Report and Order*, 35 FCC Rcd at 7628-29, para. 39. Any voice service provider that decides to block traffic from the bad actor provider must notify the Commission of its decision and provide a brief summary of its basis for making such a determination prior to initiating blocking. *Id.* at 7630, para. 42; 47 CFR § 64.1200(k)(4). If the notified voice service provider fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls, other downstream voice service providers may block the calls from the notified provider. *Call Blocking Safe Harbor Report and Order*, 35 FCC Rcd at 7630 para. 43; 47 CFR § 64.1200(k)(3)-(4). A voice service provider that decides to block traffic from the bad actor provider must notify the Commission of its decision and provide a brief summary of its basis for making such a determination prior to initiating blocking. *Id.* at 7630, para. 43; 47 CFR § 64.1200(k)(4).

¹⁴ See *Call Authentication Trust Anchor*, 36 FCC Rcd at 1905, para. 88.

¹⁵ 47 CFR § 64.6305(c). See *Call Authentication Trust Anchor*, 36 FCC Rcd at 1904, para. 86; *Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, DA 21-454 (WCB Apr. 20, 2021).

Continued origination of illegal robocalls following this notice will be used as evidence of a defective certification, and we may remove your certification from the Robocall Mitigation Database.¹⁶

Please direct any inquiries or responses regarding this letter to Jessica Manuel, Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, FCC, at jessica.manuel@fcc.gov or (202) 418-1305; and Raul Rojo, Attorney Advisor, Telecommunications Consumers Division, Enforcement Bureau, FCC, at raul.rojo@fcc.gov or (202) 418-1336 and cc: to Kristi Thompson, Division Chief, Telecommunications Consumers Division, Enforcement Bureau, FCC, at kristi.thompson@fcc.gov. A copy of this letter has been sent to the Traceback Consortium.

Sincerely,

Loyaan A. Egal
Acting Bureau Chief
Enforcement Bureau
Federal Communications Commission

¹⁶ See *Call Authentication Trust Anchor*, 36 FCC Rcd at 1902, 1905, paras. 81, 88.

ATTACHMENT A

Customer	Date of Call	Date of ITG Notification	Caller ID	Called Number	Description	Violation
National Auto Protection	Jan 17, 2022 16:38 UTC	Jan 20, 2022 15:20 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	Feb 25, 2022 15:23 UTC	Mar 11, 2022 02:25 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	Mar 01, 2022 16:17 UTC	Mar 14, 2022 14:02 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	Mar 01, 2022 17:57 UTC	Mar 11, 2022 02:24 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	Mar 01, 2022 19:40 UTC	Mar 11, 2022 02:23 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	Mar 01, 2022 20:17 UTC	Mar 14, 2022 14:01 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	May 20, 2022 19:04 UTC	May 24, 2022 13:55 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	May 20, 2022 19:07 UTC	May 24, 2022 18:16 UTC			AutoWarrantyExtend	47 USC 227(b); 47

						CFR 64.1200(a)
National Auto Protection	May 20, 2022 19:52 UTC	May 24, 2022 17:22 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)
National Auto Protection	May 20, 2022 21:48 UTC	May 24, 2022 17:48 UTC			AutoWarrantyExtend	47 USC 227(b); 47 CFR 64.1200(a)