

Kenect, LLC
1221 Valley Grove Way #400
Pleasant Grove, UT 84062

December 31, 2024

ROBOCALL MITIGATION PLAN

Introduction and Background

The Federal Communications Commission (“Commission” or “FCC”) directs voice service providers, as defined in the Commission’s rules, to upload a Robocall Mitigation Plan (“RMP”) to the Robocall Mitigation Database (“RMD”) describing specific reasonable steps by the provider to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of the RMP. The Commission rules contemplate that the provider’s plan describe how it “complies with its obligation to know its customers pursuant to § 64.1200(n)(4), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s).” 47 C.F.R. § 64.6305(d)(1)(ii). The Commission acknowledges, however, that, “we do not currently require [] providers other than gateway providers to engage in ‘know-your-upstream-provider’ procedures, [but] if they have put such procedures in place, they must be documented in their robocall mitigation plan,” and that “we do not specifically require providers to use call analytics.”¹ .

Entity Covered by RMP

Kenect, LLC (“Kenect”) (<https://www.kenect.com/>) offers a text messaging platform to business customers. Kenect offers no voice services to customers. Kenect permits a business customer to send and receive text messages to the business customer’s customers. The Commission considers text messaging information services. However, Kenect’s platform will forward voice calls from the text message recipient to each customer’s main business line upon receiving calls to the text message originating telephone number.

Kenect submits this RMP in accordance with the Commission’s rules applicable to voice service providers to the extent the Commission deems Kenect’s call forwarding feature a “voice service” as set forth in Section 64.6300(l) of the Commission’s rules, 47 C.F.R. §64.6300(l). For all voice traffic, Kenect lacks control of the network infrastructure necessary to implement the STIR/SHAKEN authentication framework. All voice traffic originating on Kenect’s network is authenticated under the STIR/SHAKEN authentication framework pursuant to 47 CFR § 64.6301(a) by either Twilio or Bandwidth as set forth below. Accordingly, Kenect performs Robocall Mitigation as set forth below in this RMP.

¹ *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, FCC 23-18, ¶ 40, n. 155-56 (2023).

STIR/SHAKEN Commitment

Pursuant to Section 64.6305 of the Commission's rules, 47 C.F.R. § 64.6305, Kenect commits to taking all such reasonable steps to avoid originating illegal robocall traffic and to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers from using Kenect service to originate calls.

Importantly, Kenect exercises no control over the relevant network infrastructure to implement the technical requirements of STIR/SHAKEN described under 47 C.F.R. §64.6301. As such, under the Commission's robocall mitigation orders, Kenect is not required to implement STIR/SHAKEN.² In fact, Kenect contracts with Twilio and Bandwidth (third-party providers) to facilitate termination of calls forwarding as a result of the customer returning calls to the originating text number as well as to obtain telephone numbers used by customers if necessary to provide text messaging services. Kenect understands that Twilio and Bandwidth obtain the necessary Service Provider Code ("SPC") Tokens and implement the various STIR/SHAKEN attestation levels and technical requirements for any voice communications resulting from call forwarding that originate on either Twilio or Bandwidth's network.

Kenect's information service requires no Operating Company Number ("OCN") nor has the National Exchange Carriers Association assigned Kenect an OCN. Kenect does not meet the requirements to receive, and has not received, an SPC Token under the Secure Telephone Identity Governance Authority's Token Access Policy.

Kenect's current operations remain subject to the indefinite STIR/SHAKEN implementation extension under 47 C.F.R. §64.6304(b). Kenect maintains no control over the relevant network infrastructure to implement the technical requirements of STIR/SHAKEN and is without the ability to obtain an SPC Token.

Know-Your-Customer

As part of the customer onboarding process, Kenect undertakes various commercially reasonable precautions to verify a given customer's identity and bona fides as part of entering into enforceable contracts with all customers. Kenect engages in a comprehensive know-your-customer registration process with Twilio and Bandwidth for each customer and phone number obtained providing Twilio and Bandwidth with the opportunity to independently verify the identity and bona fides of all Kenect customers.

² See *Call Authentication Trust Anchor, et al*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, No. 20-67, FCC 20-42, ¶ 40 (2020); see also *Call Authentication Trust Anchor*, Second Report and Order, WC Docket No. 17-97, FCC 20-136, ¶ 20 (2020).

Kenect works closely with Twilio and Bandwidth to prevent, detect, and mitigate the delivery of illegal robocall traffic. Both Twilio's and Bandwidth implemented technical and operational processes, including analytics software, to monitor all traffic on its networks.

In cases where Kenect customers calls forward through telephone numbers obtained through Twilio and Bandwidth, Kenect has a documented, verified relationship between the customer and the telephone number(s) receiving forwarded calls. The call forwarding via the Kenect platform only originates by Kenect customers using assigned telephone numbers and terminates to the customers main telephone line.

Contractual Terms and Conditions

Kenect completes the know-your-customer screening process for Twilio and Bandwidth as part of the onboarding process, and a know-your-customer registration process with each provider when obtaining numbers from Twilio for customer use. Kenect is subject to provisions in its enforceable contracts with both Bandwidth and Twilio requiring Kenect and customers transiting traffic over the provider's network to take all necessary steps to prevent illegal robocalls on the carrier's network. Kenect customers also contractually agree to various terms and conditions related to compliance with law, called/texted party consent, and acceptable use, among others, including, the following:

- Customers agree that they will only provide access to Kenect's services to any person or entity who is a customer employee or contractor and ensure that no authorized user will use Kenect's services other than in accordance with all applicable laws and regulations. Importantly, Kenect requires customers to implement and maintain the appropriate administrative, technical, and organizational measures and safeguards to prevent the loss or unauthorized use of any login credentials required to access Kenect's systems and services, and to promptly report any known or suspected loss or unauthorized use of such login credentials or any other breach of security. Customers contractually agree to bearing responsibility for any loss or unauthorized use of their login credentials and any activity occurring under a customer's account using customer's login credentials.
- Customers agree to comply with all applicable federal, state, local and other laws, ordinances, regulations, rules and codes applicable in connection with its activities including, without limitation, relating to privacy, data protection, confidentiality, and security.
- Customers agree to comply with, and ensure that each authorized user complies with, the Telephone Consumer Protection Act of 1991 and its implementing regulations, any applicable federal or state law requirements related to making or sending communications via phone call, the Telemarketing Sales Rule, mobile carrier requirements, and all applicable laws related to caller identification. Customers also agree to maintain an accurate and complete record of the status of a third party's consent, revocations of consent, and any Do Not Call obligations, including the language consented to and the date of consent and revocation, as applicable, and that all such records are retrievable.
- Customers agree and acknowledge that Kenect's services use Bandwidth or Twilio for certain voice call forwarding services, and that customers use of the services is subject to each

providers' Terms of Service and Acceptable Use Policy.

- Customers to agree that Kenect services shall not be used to violate law, regulations, governmental orders, industry standards, or telecommunications providers' requirements or guidance, and require that Kenect customers (a) obtain any required consents prior to transmitting, recording, collecting, or monitoring data or communications; and (b) comply with opt-out requests for any data or communications. Furthermore, customers agree that Kenect's services shall not be used to transmit any illegal, harmful, unwanted, inappropriate, or objectionable content.

Traceback Requests

Kenect commits to responding to traceback requests and to cooperate with investigating and stopping illegal robocalls as necessary. Kenect will respond to traceback requests received from the Industry Traceback Group, state and federal regulators, including the Commission, and law enforcement within twenty-four (24) hours as required under the Commission rules. Kenect will dedicate sufficient resources to provide timely and complete responses to such requests and will investigate suspicious activity found by its monitoring systems or reported to it by appropriate parties and take appropriate action as necessary.

Company Information

The name, title, department, business address, telephone number and email address of the individual responsible for addressing robocall-related issues for this RMP follows:

Name:	Jeff Jones
Title:	Chief Operating Officer
Department:	Executive
Business Address:	1221 Valley Grove Way, #400 Pleasant Grove, UT 84062
Telephone Number:	(801) 718-6121
Email Address:	jjones@kenect.com

CERTIFICATION

I, Jeff Jones, Chief Operating Officer of Kenect, LLC (“Kenect”), do hereby certify, under penalty of perjury, the following:

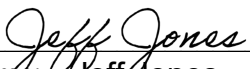
- a. Kenect lacks control over the necessary infrastructure to implement STIR/SHAKEN requirements in its network.
- b. Kenect business name and primary address follows:

Kenect, LLC
1221 Valley Grove Way #400
Pleasant Grove, UT 84062

- c. Entities owning 10% or more of Kenect include: PSG Equity (<https://www.psgequity.com>). Kenect has no subsidiaries or affiliates.
- d. Kenect has had no licenses revoked by the Commission and has not been subject to enforcement action by the Commission.
- e. Kenect operates under the corporate name Kenect, LLC.
- f. Kenect previously used or operated under any other business name, Clario.
- g. The name, title, department, business address, telephone number and email address of the individual responsible for addressing robocall-related issues for the Robocall Mitigation Plan follows:

Name:	Jeff Jones
Title:	Chief Operating Officer
Department:	Executive
Business Address:	1221 Valley Grove Way #400 Pleasant Grove, UT 84062
Telephone Number:	(801) 718-6121
Email Address:	jjones@kenect.com

- h. Kenect role in the call chain is that of a voice service provider without a STIR/SHAKEN implementation obligation to serve end users.
- i. Kenect has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. Kenect is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. Kenect has no OCN.



Name: Jeff Jones
Title: Chief Operating Officer
Date: December 31, 2024