LINQ APP INC.
ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission ("FCC" or "Commission") has adopted rules requiring voice service providers, like Linq App Inc. ("Linq App"), to, among other things, file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database ("RMD"). 47 CFR § 64.6305; *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023) ("*Sixth Caller ID Authentication Report and Order*").

The FCC requires that all voice service providers certify in the Commission's RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that it originates, carries or processes are subject to a robocall mitigation program consistent with the Commission's rules.[1] The provider's mitigation plan "shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours 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 that use its service to originate calls." 47 C.F.R. § 64.6305(a)(2).

Despite imposing a general duty to mitigate "robocalls," the Commission's codified rules do not define "robocall."[2] The TRACED Act defines "robocall violation" as "a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934." TRACED Act § 11(d), Pub. L. No. 116-105, 133 Stat. 3274 (2019); *id*. at § 13(d)(f)(3) (defining a "suspected unlawful robocall" as a "call that the Commission or a voice service provider reasonably believes was made in violation of subsection (b) or (e) of section 227 of the Communications Act of 1934." Thus, Linq App's

[1] *See* https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf (WCB Jan. 25, 2024 Public Notice).

[2] The Commission's TCPA-related regulations, 47 C.F.R. § 64.1200, use the undefined term "illegal traffic,"47 C.F.R. § 64.1200((k)-(m)), while its STIR/SHAKEN-related regulations define the FCC's public-facing Robocall Mitigation Database, but not the "robocalls" that are to be mitigated. 47 C.F.R. § 64.6300. Thus, neither of the regulations that bear directly on the project of robocall mitigation expressly define "robocall." *Cf. In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rule Making, 32 FCC Rcd. 9706, 9725 ¶ 56 (Nov. 17, 2017) (declining to define "illegal robocall," and acknowledging that "the record shows confusion regarding how the proposed definition of 'illegal robocall' should apply to the call blocking rules."); *In re Core Communications, Inc., et al. Tariff F.C.C. No. 3*, WC Docket No. 21-191, Order, 36 FCC Rcd. 9997, 9999 (June 23, 2021) (In a related context, stating that the "Commission defines a robocall as a call made using an automatic telephone dialing system or an artificial or prerecorded voice.") (citing 47 U.S.C. § 227(b)(1); 47 CFR § 64.1200(a)). Linq App therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

training and mitigation efforts focus, as they must, on potentially unlawful calls that violate either (a) 47 U.S.C. § 227(b) (governing non-emergency calls initiated with a prerecorded or artificial voice or an automatic telephone dialing system, as that term has been interpreted by the Supreme Court in *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2001)) or (b) 47 U.S.C. 227(e), or the Truth in Caller ID Act, which prohibits people from causing "any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value," absent an applicable exemption.

The FCC's rules contemplate that the provider's plan should 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 any 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 has acknowledged, 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." *Sixth Caller ID Authentication Report and Order* ¶ 40 & n.155-56.

The Commission has explained that a robocall-mitigation program is "sufficient if it includes detailed practices that can reasonably be expected to significantly reduce" the provider's origination or carriage of illegal robocalls, and the voice service provider complies with the practices described in its plan. *Sixth Caller ID Authentication Report and Order* ¶ 31. Linq App is dedicated to developing and taking reasonable steps. This document outlines Linq App's robocall mitigation plan.

II. Linq App's Know Your Customer ("KYC") Standards

Linq App is a voice service provider that focuses its business and operations on the business segment of the voice services communications market, with an emphasis on advanced communications offerings in the UCaaS space. As part of its customer-onboarding process, Linq App undertakes various commercially reasonable precautions to verify a given customer's identity as part of entering into a service agreement.

Among other data points collected and, as appropriate, verified, as part of those KYC and onboarding processes, Linq App gathers the following customer-identifying facts and circumstances:

- Customer business name,
- Customer state of incorporation and EIN,
- Customer physical business location,
- Name, phone number and email address of Customer contact person(s), and
- Confirmation the Customer has not been the subject of an adverse final

determination in an adjudicatory proceeding brought by either a private or government party, including any FCC order, court order, or other similar determination, for violating any state or federal laws or Commission Rules pertaining to robocalls.

Linq App does not serve wholesale carrier customers. If it does, however, Linq App acknowledges that its verification practices would be expanded to include confirming a carrier customer's reported status in the FCC's Form 499 Filer database of registered carriers, and the Commission's Robocall Mitigation Database, along with a completed USF exemption certificate, if and as applicable.

III. Linq App's Acceptable Use Policy

Linq App's end users must comply with Linq App's Acceptable Use Policy (AUP). Among other things, this AUP prohibits:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
- Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including, without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. § 227), the Federal Communications Commission regulations (47 C.F.R. § 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, and all federal and state Do Not Call and calling-time restriction laws and regulations.
- Creating a false identity, forged email address or header, phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act.

Linq App reserves the right to suspend and/or terminate all Services in the event of an AUP violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

Linq App is a non-facilities-based reseller that lacks the necessary facilities and control over the network infrastructure necessary to implement STIR/SHAKEN, and therefore does not have a STIR/SHAKEN implementation obligation. *See Sixth Caller ID Authentication Report and Order* ¶ 36 & n. 137; *id*. ¶ 45 & n.170.

Linq App's end users only use telephone numbers to which they have subscribed from (or ported into) Linq App, such that Linq App has a documented, verified relationship between the originating end user and their telephone number(s) used to originate their calls. Thus, it should be technically impossible for Linq App's end users to manipulate their caller ID to violate the Truth in Caller ID Act. Should that change and customers could use as a caller ID any number not assigned by Linq App, or ported into Linq App's network by the end user, Linq App will document the end user's right to use the associated phone number(s) from the unaffiliated provider.

V. Proactive Network Monitoring

Linq App has various monitoring and reporting systems in place via its upstream carrier to analyze traffic on its network for potentially suspicious traffic patterns that are likely to be associated with illegal robocalls or other potentially unlawful usage. For example, Linq App's underlying carrier provider and monitoring systems can assess traffic based on various criteria, including data relating to call frequency per line, concurrent-call count, short-duration calls, answer-seizure ratios, and other anomalous call patterns. Linq App does not currently use any third-party vendors for robocall mitigation or analytics tools.

If those systems and/or Linq App detects a pattern consistent with illegal robocalls, or it has reason to suspect illegal robocalling or spoofing is occurring on its network, Linq App will take prompt action to identify the party that is using its network to carry these calls and take appropriate action. Once suspected unlawful traffic is discovered, Linq App will block any further traffic from being carried from the customer account associated with that suspicious traffic. In the event Linq App discovers any suspicious traffic that is not demonstrably unlawful, Linq App will complete its investigation, and their service can be temporally suspended while that process is completed depending on the severity of the complaint.

VI. Commitment to Timely Traceback Responses and Cooperation

Linq App commits to respond fully and in a timely manner, within 24 hours, 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 that use its service to originate, carry, or process illegal robocalls. Linq App 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.