

EZZI TELCO LLC ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like EZZI TELCO LLC (“EZZI TELCO”), 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); *id.* at § 64.6305(b)(2)-(c)(2) (parallel rule for gateway and non-gateway intermediate providers’ “carrying or processing illegal robocall traffic”).

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

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)). EZZI TELCO therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress expressly addressed.

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, EZZI TELCO’s 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) [for originating voice service providers], 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); *see also* 47 C.F.R. §64.6305(f)(2)(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. EZZI TELCO is dedicated to developing and taking reasonable steps. This document outlines EZZI TELCO’s robocall mitigation plan.

IIa. EZZI TELCO’s Know Your Customer (“KYC”) Standards

EZZI TELCO is a voice service provider and wholesale, intermediate (both gateway and non-gateway) provider that focuses its business and operations on retail consumer and business users and wholesale voice services communications markets. EZZI TELCO has revisited and applied its KYC criteria related to its current customers to be sure that they all meet the same KYC Standards that we require for new customers. As part of its customer-onboarding process, EZZI TELCO undertakes various commercially reasonable precautions to verify a given customer’s identity, including having its customers complete a KYC questionnaire, a USF Exemption Certificate for carrier customers, and a formal written contract. Among other data points collected and, as appropriate, verified, as part of those processes, EZZI TELCO gathers the following customer-identifying facts and circumstances:

- Customer business name and entity type,
- state or country of incorporation,
- physical business location,
- contact person(s), with business phone number and email addresses, for main, technical, and compliance customer contacts;
- trade and/or bank references,

- federal tax ID number,
- FCC 499 Filer ID & FRN;
- Robocall Mitigation Database filing indicating STIR/SHAKEN compliance; and
- Company website and/or other customer-facing presence;

EZZI TELCO's verification practices 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, and performing internet research into the company's reasonably accessible online profile and potential call-usage-claim-related history. EZZI TELCO also conducts, as applicable, reference checks with a prospective customer's other carrier-suppliers, and reviews their traceback history. When EZZI TELCO onboards new customers, EZZI TELCO's team also checks all new account traffic profiles for patterns relating to call duration, caller ID usage, ASR, and other metrics to help assess traffic hygiene issues.

IIb. Enhanced KYC, Traffic Monitoring and Mitigation Procedures

EZZI TELCO applies KYC procedures to both new and existing customers. New customers are vetted using corporate documents, tax IDs, FCC registrations, RMD status, business addresses, references, websites, and compliance contacts before activation.

Existing customers are periodically reviewed to confirm FCC Form 499 registration, RMD compliance, and operational legitimacy. Customers with unusual traffic patterns may be subject to enhanced review.

EZZI TELCO does not currently utilize a third-party robocall analytics vendor. Instead, it performs internal monitoring using CDRs, routing information, network statistics, and operational reports. Monitoring includes abnormal call volumes, short-duration calls, sequential dialing, high attempt rates, ASR anomalies, excessive failures, caller ID irregularities, newly onboarded customer traffic, and traceback-related traffic.

When suspicious traffic is detected, EZZI TELCO may request explanations and documentation, require proof of consent, increase monitoring, restrict or block traffic, suspend or terminate service, and cooperate with traceback requests, law enforcement, and industry investigations. Management review is required for suspected unlawful robocall or spoofing activity, and the Company continuously evaluates additional mitigation technologies and best practices.

III. EZZI TELCO's Acceptable Use Policy

As part of its customer-onboarding process, all of EZZI TELCO's customers contractually agree to various terms and conditions, including a commitment to comply with EZZI TELCO'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, such as 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.

EZZI TELCO's contracts with its customers provide that EZZI TELCO is authorized to suspend and/or terminate all Services in the event of an AUP violation.

IV. Telephone Number Authorization and Future STIR/SHAKEN Implementation

At this time, EZZI TELCO has not implemented the STIR/SHAKEN authentication framework on any portion of its network. EZZI TELCO is, however, committed in good faith to pursuing future STIR/SHAKEN implementation and related carrier coordination as part of its ongoing compliance efforts. EZZI TELCO is in the process to apply for its OCN from NECA and intends to continue the STI-PA implementation process with iconectiv. Once the STI-PA process is complete, EZZI TELCO will contract with a Certified Authority for the tokens and will complete the necessary onboarding and operational requirements to be fully Stir/Shaken compliant.

EZZI TELCO restricts its end users to only making calls from telephone numbers that EZZI TELCO has assigned to them or numbers they have demonstrated a right to use. EZZI TELCO further prohibits unlawful caller ID spoofing and unauthorized prerecorded/artificial voice calling activity through its contractual restrictions, monitoring efforts, and acceptable use policies.

V. Proactive Network Monitoring

EZZI TELCO is working to implement various monitoring and reporting systems in place 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, EZZI TELCO's monitoring systems is in development to assess and, as applicable, flag or automatically block, traffic based on various criteria, including

- ▢ matching NPA-NXXs of the calling and called parties' telephone numbers;
- ▢ blocking calls purporting to be from a telephone number on a Do-Not-Originate list;
- ▢ blocking calls from any Media IP address associated with a known or reported illegal robocalling entity.

If EZZI TELCO detects a pattern consistent with illegal robocalls, or has reason to suspect illegal robocalling or spoofing is occurring on its network, EZZI TELCO takes prompt action to identify the party that is using its network to carry these calls and take appropriate action.

VI. Commitment to Timely Traceback Responses and Cooperation

EZZI TELCO 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. EZZI TELCO 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.