



EZYTEL SOLUTIONS
ROBOCALL MITIGATION PROGRAM

February 2024

BACKGROUND

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like EYZTEL SOLUTIONS to, among other things, file certifications and robocall mitigation plans (RMP) 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, by February 26, 2024, 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(c)(2) (parallel rule for 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

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)). EYZTEL SOLUTIONS therefore focuses on the two types of unlawful calls—227(b) and 227(e) of the TCPA—that Congress

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, EZYTEL SOLUTIONS’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.

By design, EZYTEL SOLUTIONS’s services are provisioned in a manner to prevent its end users from violating either of these subsections of the TCPA. First, its system is incapable of generating the telephone numbers its end users may use EZYTEL SOLUTIONS’s voice services to call. Like traditional phone service, EZYTEL SOLUTIONS’s end users must supply and choose the phone numbers it calls with EZYTEL SOLUTIONS’s service. Second, EZYTEL SOLUTIONS’s end users must make live-agent calls; EZYTEL SOLUTIONS’s services are not compatible with using prerecorded or artificial voice calls (any more than a traditional desk or home phone would be). As such, 47 U.S.C. § 227(b) violations simply should not, and in our experience do not, occur via EZYTEL SOLUTIONS’s services. And, third, EZYTEL SOLUTIONS’s end users can only use caller IDs that they have been assigned by EZYTEL SOLUTIONS as their outbound caller ID, such that, absent some hacking event, which would violate EZYTEL SOLUTIONS’s AUP, EZYTEL SOLUTIONS’s end users can’t manipulate their caller ID. Thus, by design, EZYTEL SOLUTIONS’s end users are likewise prevented from using EZYTEL SOLUTIONS’s services to violate 47 U.S.C. § 227(e).

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

expressly addressed.

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. As illustrated in this plan, EZYTEL SOLUTIONS is dedicated to developing and taking reasonable steps, consistent with FCC regulations and its “[Best Practices](#)” guidance. This document outlines EZYTEL SOLUTIONS’s robocall mitigation plan.

COMPANY SUMMARY

EZYTEL SOLUTIONS is an intermediate provider that focuses its business and operations on the wholesale and business customer segments of the voice services communications market.

ROBOCALL MITIGATION PLAN (RMP)

As EZYTEL SOLUTIONS’s network may serve as a Non-gateway Intermediate Provider, and/or a Gateway Provider, the following RMP describes EZYTEL SOLUTIONS’s affirmative and effective measures to prevent customers from originating illegal robocalls. The following measures are consistent with the FCC’s *Sixth Caller ID Authentication Report and Order* and the [Gateway Provider Report and Order](#).

As a Gateway Provider, EZYTEL SOLUTIONS commits to play a more active role in the fight against illegal robocalls originating from overseas by, among other things, applying STIR/SHAKEN caller-ID to all Session Initiation Protocol (SIP) calls carrying a U.S. number, submitting this current RMP version, instituting mandatory blocking in certain instances, committing to a 24-hour response time to traceback requests from the Industry Traceback Group (ITG), implementing “know your upstream provider” and blocking calls based on a reasonable Do Not Originate (DNO) as describes bellow:

**A) Affirmative, effective measures to prevent customers from
originating illegal robocalls.**

1. Call Authentication Mechanism:

EZYTEL SOLUTIONS has Fully Implemented STIR/SHAKEN (Secure Telephone Identity Revisited/Signature- based Handling of Asserted Information Using Tokens) protocols for call authentication (**§ 64.6301 Caller ID authentication**) This ensures that caller ID information is authenticated, reducing the prevalence of spoofed numbers.

2. Know-your-Upstream Provider Protocol:

EZYTEL SOLUTIONS has implemented appropriate Know Your Customer (KYC) protocols when onboarding new customers.

As part of its customer-onboarding process, EZYTEL SOLUTIONS implements several measures to confirm the identity and relevant business practices of a potential customer before entering into a formal agreement with them. This KYC Protocol outlines the procedures for collecting and verifying customer information to ensure compliance with regulatory standards and mitigate risks associated with new and existing customers.

All prospective customers must complete the following a KYC Protocol which provides EZYTEL SOLUTIONS with detailed background, business, and regulatory compliance details, as well as customer references about the potential customer:

2.1 KYC Form Submission: Customers are required to complete and submit a KYC Form containing the following information. Failure to comply with KYC requirements may result in delays or rejection of the interconnection request.

The KYC Form must be filled out in its entirety for acceptance.

a) Business Information

- Type of Business
- Types of voice services provided.
- Contact information: Main Telephone No, Address, emails,

- Employees contact information: telephone numbers, emails, LinkedIn profile, job position.
- FCC 499 File ID No
- FCC Registration No (FRN)
- Federal Tax ID No (FEIN) or equivalent
- Universal Service Fund (USF) registration number

b) Business Purpose, Activities and Regulatory Compliance: This includes questions such as:

- Do you originate calls?
- Do you act as a US point of entry (Gateway provider) for foreign originated traffic?
- Do you have a Subscription Account Number for accessing the National Do Not Call Registry?
- Does your business involve telemarketing to solicit the purchase of goods, services, or charitable contributions?
- Tracebacks request history information
- Have you been determined by ITG to be a "Non-Cooperative Voice Service Provider
- Do you have a Robocall mitigation plan in place to combat illegal Robocalling, including customer vetting and telephone number validation?
- Have you implemented STIR/SHAKEN in your network?
- NECAS's Operating Company Number (OCN):

c) Bank and Trade References: EYZTEL SOLUTIONS requests 2 bank and trade references per Customer on each KYC Form

d) Acknowledgment: By submitting the KYC Form and associated documents, clients acknowledge their understanding and agreement to comply with the requirements outlined in this KYC Form.

2.2 KYC Form Validation Process: Upon receipt of the required information in the KYC Form, EYZTEL SOLUTIONS conducts a validation process to ensure the accuracy of the information provided by the Customer. The validation process includes:

- Reviewing the client's website, social media profiles, and LinkedIn profile.
- Verifying the validity of provided phone numbers.

- Confirming the authenticity of FCC 499 Filing and FCC registration numbers.
- Checking for registration in the Robocall Mitigation Database (RMD)
- Customer's provided information is cross-checked for consistency with the data uploaded in the Robocall Mitigation Database

If the prospect is not in compliance, EYZTEL SOLUTIONS will decline to move forward.

2.3 Record Keeping: The Company maintains records of all KYC Forms, validation processes, and KYC Protocols for auditing and regulatory purposes.

3. Mandatory Blocking Following Commission Notification

As a Gateway Provider, EYZTEL SOLUTIONS will promptly investigate and block illegal traffic upon receiving a notice from the Commission's Enforcement Bureau. Additionally, EYZTEL SOLUTIONS will adhere to the specified *Process for Issuing a Notification of Suspected Illegal Traffic* outlined in the *Gateway Provider Report and Order* to ensure effective resolution of such issues.

4. Only Accepting Traffic from Providers in the RMD

In accordance with 47 C.F.R § 64.6305(e)(1), EYZTEL SOLUTIONS only accepts calls from Providers listed in the RMD:

- **Domestic Voice Service Providers:** As per 47 C.F.R § 64.6305(e)(1), EYZTEL SOLUTIONS solely accepts calls from domestic Voice Service Providers if the provider's filing is listed in the RMD and has not been subject to delisting due to enforcement actions.
- **Foreign Voice Service Providers and Foreign Intermediate Providers:** EYZTEL SOLUTIONS only accepts calls from Foreign Voice Service Providers or Foreign Intermediate Providers utilizing North American Numbering Plan upon the provider's inclusion in the RMD and absence of delisting due to enforcement actions.
- **Gateway Providers:** EYZTEL SOLUTIONS will only accept calls directly from Gateway Providers if the provider's filing: (a) is listed in the RMD, (b) demonstrates affirmative submission of the filing, and (c) has not undergone delisting due to enforcement actions.

5. Contractual Provisions to Mitigate Illegal Robocalls

For U.S. commercial clients, EYZTEL SOLUTIONS requires the execution of a Master Service Agreement (MSA). This MSA, provided by EYZTEL SOLUTIONS, includes a termination clause among other provisions, specifying consequences for non-compliance with federal, state, and local laws, regulations, or rules related to the use of EYZTEL SOLUTIONS services or equipment. EYZTEL SOLUTIONS customers agree to various terms and conditions, including compliance with EYZTEL SOLUTIONS Terms of Use. These terms, among other things, prohibit:

- 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 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.
- Using EYZTEL SOLUTIONS Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices, and Short Code Monitoring Handbook.
- 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. EYZTEL SOLUTIONS contracts with its customers stipulate that it is authorized to suspend and/or terminate all Services in the event of an AUP violation.

6. Proactive Network Monitoring:

EYZTEL SOLUTIONS has 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, EYZTEL SOLUTIONS's monitoring systems can assess traffic

based on various criteria, including data relating to short-duration calls, answer-seizure ratios, invalid Caller ID ANIs, and anomalous volumes of 404, 503 and other call-failure codes. If EYZTEL SOLUTIONS detects a pattern consistent with illegal robocalls or has reason to suspect illegal robocalling or spoofing is occurring on its network, EYZTEL SOLUTIONS takes 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, EYZTEL SOLUTIONS blocks any further traffic from being carried associated with the Media IP address of that suspicious traffic.

7. Call Filtering and Blocking:

EYZTEL SOLUTIONS utilizes a variety of network tools to combat illegal robocalls. Specifically, and pursuant to rules adopted by the Commission in FCC 17-151, EYZTEL SOLUTIONS blocks calls from phone numbers on Do- Not-Originate (“DNO”) list from SOMOS. EYZTEL SOLUTIONS has the ability of blocking calls from non-LERG ANIs, invalid and wireless numbers.

EYZTEL SOLUTIONS utilizes RoboGuard to block media IPs reported as being associated to scam calls, FCC or CLEC complaints.

If a call comes from a “Neighboring” number, meaning the NPA-NXX is the same on both the ANI and DNIS, such call will be blocked.

Caller ID Blocking Tool (CDI) – The system monitors CDI profiles for low Answer Seizure Ration (ASR), low Average Length of Call (ALOC), high Short Duration Percentage (SDP), if an ANI reaches the set threshold, the ANI will be blocked.

Traffic received with an S/S token will be passed and will not be altered. EYZTEL SOLUTIONS is actively blocking traffic received without an S/S token.

B) Traceback Process and Best Practices

Following USTelecom’s Traceback Process and Best Practices, EYZTEL SOLUTIONS diligently follows established protocols to address and respond to traceback requests. These practices emphasize the importance of prompt and thorough cooperation in identifying the origins of illegal robocalls and taking appropriate action to mitigate their impact. By adhering to these industry standards, we demonstrate our commitment to combating unlawful telecommunications activities and upholding the integrity of our services. Our adherence to these following best practices ensures effective collaboration with industry stakeholders and regulatory authorities in combating the

scourge of illegal robocalls, thereby enhancing trust and reliability within the telecommunications ecosystem:

- **24 Hours response:** EYZTEL SOLUTIONS commits to respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities to investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocall, in accordance with applicable laws.
- **Dedicated Point of Contact:** EYZTEL SOLUTIONS has designated a dedicated point of contact for addressing requests from other Voice Service Providers or USTelecom related to Suspicious Traffic. This person will oversee all matters regarding robocall mitigation actions.
- **Ongoing Coordination:** EYZTEL SOLUTIONS will exchange information regarding suspicious traffic with other VSP and USTelecom through email, phone calls, etc.

C) Formal Investigations

- EYZTEL SOLUTIONS receive correspondence from the Enforcement Bureau dated January 26, 2023. The correspondence informed EYZTEL SOLUTIONS of an investigation related to potential violations of the TCPA and the Commission's rules governing prerecorded messages. It instructed EYZTEL SOLUTIONS to provide certain documents responsive to an enclosed subpoena. EYZTEL SOLUTIONS responded to the subpoena on March 9, 2023. EYZTEL SOLUTIONS has not received further correspondence from the Commission regarding its investigation and assumes the matter is closed.
- EYZTEL SOLUTIONS received a notice from the Social Security Administration in 2022 in which the Administration alleged that SSA-related scam calls traversed EYZTEL SOLUTIONS's network. EYZTEL SOLUTIONS complied with the Notice's requirements and provided all requested documentation. The parties entered into a settlement agreement dated January 13, 2023 by which the parties settled all claims between them. No finding of actual wrongdoing was ever made.
- EYZTEL SOLUTIONS received a Civil Investigative Demand from the Indiana Attorney General dated August 1, 2022 which indicated that EYZTEL SOLUTIONS may have violated the Telemarketing Sales Rule, the Telephone Consumer Protection Act and various Indiana statutes. EYZTEL SOLUTIONS timely objected to the issuance of the CID in correspondence

dated August 29, 2022. EZYTEL SOLUTIONS has not received further communication and assumes the matter is closed.