

YTEL INC

ROBOCALL MITIGATION PLAN

Pursuant to 47 C.F.R. § 64.6305, Ytel, Inc. (“Ytel”, “the Company”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls.

This document describes the practices and procedures which Ytel has in place to protect its business customers and to mitigate illegal robocalls. Ytel may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

Ytel has not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, and none of its prior certifications have been removed from the Database by the Commission.

Ytel has not been, at any time in the prior two years, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with the Company’s findings of actual or suspected wrongdoing due to it transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

The Ytel, leadership is driven by a singular mission and that is to revolutionize the way businesses and teams within those business enterprises communicate and succeed. The Ytel journey began in 2012 with a deep understanding of the challenges faced in the direct response and contact center industries. And to create a platform that would not only streamline communications but also magnify the impact of sales efforts. Leadership’s commitment to this mission led to the development of a carrier-grade network that serves as the backbone of the Ytel innovative communication suite which is offers to business customers.

Ytel is registered with the Federal Communications Commission (“FCC”) and holds the 499 Filer ID number of 829481. The Company’s FRN/CORESID Number is 0022139232.

THE COMPANY PRIMARY PLACE OF BUSINESS

Address: 26632 Towne Centre Dr. Suite 300
Lake Forest, CA, 92610
Phone: (800) 382 - 4913
Website: Ytel.com

Leaders of the company are:

CEO

Name: Nick Newsom

Address: 26632 Towne Centre Dr. Suite 300

City, State, Zip: Lake Forest, CA,
92160

Phone: 9493101364

Direct Dial: 9493101364

Email Address: Nick@ytel.com

COO

Name: Brian Keep

Address: 26632 Towne Centre Dr. Suite 300

City, State, Zip: Lake Forest, CA,
92160

Phone: 9498121409

Direct Dial: 9498121409

Email Address: Brian@ytel.com

CTO

Name: Matt Grofsky

Address: 26632 Towne Centre Dr. Suite 300

City, State, Zip: Lake Forest, CA,
92160

Phone: 9493518878

Direct Dial: 9493518878

Email Address: Matt@ytel.com

Designated RMD Contact

Name: Evan Clark

Address: 26632 Towne Centre Dr. Suite 300

City, State, Zip: Lake Forest, CA,
92160

Phone: 8003824913

Direct Dial: 9498423767

Email Address: evan@ytel.com

STIR/SHAKEN COMPLIANCE (ROLE IN THE CALL CHAIN)

The Company has its own switch, IPES OCN and strong relationships with Sansay and its underlying upstream carriers such as Intelliquent, Bandwidth, and Wavecall to support the Company's Call Authentication process with the implementation of its digital certificate.

The Company only uses upstream providers that are listed in the RMD and maintains a robust

fraud detection system. In addition, any upstream provider must possess the ability to connect, in real time, with the Company so that issues with calls being processed by the Company can be immediately identified and addressed.

The Company is capable of authenticating the calling party's relationship with the caller ID ascribed to a given call to identify the Company customers. The Company's network is also more than capable of accepting and accurately transmitting all STIR/SHAKEN-related data it receives in the call path using its IPES OCN code, digital certificate and additionally applications and tools.

All DID's on the network system are provisioned for the YTel customer and the Company only provides DID's to fully vetted customers (please note the Know Your Customer Section in this document to understand how Ytel fully vets a customer).

As mentioned above all of Company CIC's are associated with the Company's IPES OCN Code. Essentially when a vetted customer sends a call, and the Company verifies the number as belonging to the Company it then goes to the signing system and is signed with a level A Attestation. The signed invite then goes to our intermediate carriers who also verify that the signing is correct.

Alternatively, if the Company is unable to verify the number it is fully rejected. If it is not Ytel's it is rejected.

KNOW YOUR CUSTOMER & ACCEPTABLE USE POLICY

Ytel is engaged in a business-to-business sales model and screens all new customer opportunities. All of our customers have corporate offices in the United States. Existing numbers are ported into one of our upstream carriers and only terminate or originate calls with Tier 1 Carriers that all have their own internal robocall mitigation processes and protocols.

All Ytel active customers have access to tools for call screening and can block calls by using CallerID details through Neustar and other solutions that Ytel provides to business customers.

Ytel performs a thorough reputation check on each of its customers and verifies the following information: legal business name, legal form of business, federal tax ID, nature of the business, primary contact person, service address, and secretary of state listing.

Not only does Ytel have a rigorous intake and Onboarding process where it secures extensive information for Customers but all relationships between Ytel and customers are governed by an MSA and EULA. The MSA/EULA specifically states the business customer is not able to resell any services sold to the customer by Ytel.

Ytel conducts due diligence on new and renewing customers, confirming the customer's identity and, business information such as Secretary of State listing. Ytel confirms the service address for all customers.

- Ytel verifies customer's business reputation prior to providing service.

- Ytel verifies customer information when contracts are renewed or services are added.
- Ytel verifies the customer's identity and their right to use the telephone number presented on calls.
- Ytel has a specific Acceptable Use Policy ("AUP") which define all Company the policies regarding the circumstances by which Ytel will deny, suspend or terminate service to a customer.

When the Company commences operations with a customer, the Company verifies all new customers with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. The Company severely limits the capabilities of new accounts until these appropriate processes are complete.

Additionally, as mentioned above all Company customers are required to agree to, and; are contractually bound by Ytel strict policies, contractual terms and conditions and a Company Acceptable Use Policy ("AUP") prohibiting the act of fraudulent voice activity as a condition of doing business with Ytel.

If any customer is found to be in possible and/or or actual violation of any Company policy as it relates to suspicious traffic and/or possible fraud, the Company has the right to immediately halt, cease and/or suspend the customers account or associated telephone numbers.

In part the Company's Terms and Conditions: Acceptable use Provisions specifically state the rights of the Company and the steps it may take regarding violation of prohibited use of the service as noted in italics.

RISK ASSESSMENT & MEASURES TO PREVENT ILLEGAL ROBOCALLING

Presently and also on an ongoing basis the Company always employs real-time controls on traffic. All calls have valid caller-ID values and ANI. Each customer has a concurrent call limit commensurate with the traffic description provided and stated in the Customer Agreement and Service Order; as applicable.

Ytel certifies that it will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls, Ytel certifies that all voice traffic which originates on its network is subject to this robocall mitigation program.

Call Record Monitoring:

The Company processes Call Detail Records ("CDR's) by exporting the data from the its switch. These CDR's can be used at anytime to help identify the potential of illegal originating robocalls. The CDR's can be analyzed and summarized to immediately notate traffic that has the characteristics of illegal originating robocall traffic. The monitoring includes High Volume, Short Duration ("HVSD"), sequential dialing patterns, calls to NPA-NXXs that may not be assigned by the North

American Numbering Plan Administrator and other best practices Ytel leadership has identified relative to the to combat identifying illegal robocalls.

The Company has designed, developed and deployed monitoring, diagnostics and analytical tools as part of the Company's network infrastructure and switching protocols. These analytical and diagnostic tools provide detailed call traces suitable for the Company to diagnose, monitor and collect data associated with calls traversing the network. When the monitoring, diagnostics and analytical tools are enabled on the Company's platform, traces are recorded for all calls and transferred to an external database for future review. These traces do not have to be individually enabled on particular lines or subscribers and are always active.

When investigating suspicious traffic, the Ytel technical team will use tools and analytics which are database driven to search for traces on particular lines or Customers and to view the traces. The tool the company employs also allow traces to be printed or exported for offline storage for further evaluation if required. The traces include decoded signaling messages, routing and number validation events, call service actions/decisions, codec selection, echo cancellation programming, media events such as digit and tone detection, tone generation, and digit out-pulsing, billing records and concise call logs. This collection of data allows for a comprehensive ability to monitor network traffic.

This monitoring is conducted when and as appropriate in accordance with the Company's best practices and also when a Customer is suspected possible nefarious calling activity.

The Company also utilizes a combination of tools in conjunction with its underlying carriers and platform providers along with third-party solutions to check for Do Not Originate (DNO) numbers. As mentioned, the Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

If the Company's monitoring process identifies the potential of illegal robocalls originating from the network, the Company will follow the internal policy and procedure and shall immediately halt, cease, suspend or terminate the Customer and of course the offending numbers and associated calling traffic.

UPSTREAM CARRIERS/CARRIER PARTNERS

The Company only uses upstream providers that are listed in the RMD and maintains a robust fraud detection system. In addition, any upstream provider must possess the ability to connect, in real time, with the Company so that issues with calls being processed by the Company can be immediately identified and addressed.

The Company provides its services to direct end user business and enterprise customers. The Company has its own switch and relationships with Sansay, iConectiv and other organizations that support the Company's STIR/SHAKEN implementation and compliance. Ytel also has relationships with upstream providers/underlying carriers with which it is interconnected. The main carrier partners/vendors with which the Company is interconnected are:

Company Name: (E.g., SiIntelligent/Bandwidth). Intelligent
Address: 1 N Wacker Dr, Suite 2500
City, State, Zip Code: Chicago, IL, 60606
General website address: <https://portal.intelligent.com/>
General Phone Number: 8663887258
General email address: support@intelligent.com

Company Name: (E.g., Sinch/Intelligent/Bandwidth). Bandwidth
Address: 2230 Bandmate Way
City, State, Zip Code: Raleigh, NC, 27607
General website address: <https://www.bandwidth.com/>
General Phone Number: 8008085150
General email address: support@bandwidth.com

Company Name: (E.g., Sinch/Intelligent/Bandwidth). Wavecall
Address: 8 The Green STE A
City, State, Zip Code: Dover Delaware 19901
General website address: <https://wavecall.net/>
General Phone Number: 8887217662
General email address: info@wavecall.net

TRACEBACK

Ytel is committed to respond within 24 hours to any and all requests from CALEA, the Industry Traceback Consortium, and all law enforcement agencies who officially and properly subpoena customer records.

Ytel is committed to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robo-callers that it learns are using our service to originate calls or transit calls into the United States and territories.

The Company commits to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. The Company shall cooperate with these groups to investigate and stop any illegal robo-callers from using the Company's service to carry or process illegal calls.

When notified by the FCC's Enforcement Bureau, Company shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis when Company receives actual written notice of such traffic from the Enforcement Bureau. The Company shall provide the Enforcement Bureau with an explanation as to why Company reasonably

concluded that the identified traffic is not illegal, and what steps it took to reach that conclusion.

As mentioned above, the Company utilizes a combination of tools provided by its underlying carriers and platform providers along with third-party solutions to check for Do Not Originate (DNO) numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

COMPANY DECLARATION

The Company certifies that it has never been under investigation or committed any violations within the last two years with any local, state, or Federal agency or equivalent related to telemarketing or robocalling. Additionally, the Company is not currently subject to a formal action or investigation due to suspected unlawful robocalling or spoofing.

If Company business changes a designated Company representative only will update this RMP as appropriate.