

## **The Champaign Telephone Company (dba CT Comm)] Robocall Mitigation Plan**

This Robocall Mitigation Plan is submitted by The Champaign Telephone Company (dba CT Comm) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all “voice service providers” to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

### **I. STIR-SHAKEN IMPLEMENTATION STATUS**

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR-SHAKEN implementation is as follows:

- The Provider has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a)(1) and (2). In addition, the Provider has established the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider’s service to originate illegal robocalls.

Presently, the Provider relies on the continuing extension from STIR-SHAKEN implementation provided under 47 CFR § 64.6304 (d) which exempts from STIR-SHAKEN Caller ID Authentication those portions of a voice service provider network that rely on technology which is unable to initiate, maintain, carry, process, and terminate interconnected VoIP calls. More specifically, at this time not all of the Provider’s existing network facilities are IP and capable of initiating, maintaining, carrying, processing, or terminating interconnected VoIP calls, with a continued transmission of STIR-SHAKEN attestation data. All VOIP traffic implements STIR-SHAKEN protocols. TDM voice traffic is monitored via TransNexus’ Clear IP RoboCall mitigation service.

### **II. TRACEBACK REQUESTS**

As noted above, the Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from

the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will going forward include within its carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated.

### **III. *CUSTOMER VETTING PRACTICES***

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all of its voice service subscribers, whether a retail or business/commercial subscriber (including any entities that are purchasing the Provider's services for resale). The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a business relationship. Generally, the Provider looks to confirm the identify of customers using its voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Provider efforts to vet retail and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider's required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at the Provider's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit. The Provider also understands the special importance of vetting any wholesale customers it may have. If necessary, the Provider may vet identity information for its wholesale customers by confirming whether the customer is an FCC Form 499-A filer in the FCC Form 499-A Filer database or in the FCC's Intermediate Provider Registry. If the customer is not registered within those databases further investigation is conducted to better understand the nature of the customer's business.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where the Provider identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within eight

(8) hours for further investigation and possible action regarding their subscribed to voice service.

#### **IV. TELEPHONE NUMBER VALIDATION PRACTICES**

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner. Further, for: (1) single line voice service subscribers, both services connected via TDM or IP, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) subscribers with multi-line telephone systems, for both services connected via TDM or IP, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities enable an automated and secure method of validating originating telephone numbers.

#### **V. INTERNATIONAL CALL ORIGINATORS**

The Provider is not currently an international voice services provider. If at any time the Provider does sell its services to customers which are international call originators using North American Numbering Plan resources it will familiarize itself with and develop best practices for fulling vetting such customers and performing telephone number validation on all international originated calls.

#### **VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES**

As a rural provider of voice services, the number of upstream providers used by the Provider to receive and deliver its originated voice calls for termination are somewhat limited. The Provider has longstanding relationships with these upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, the Provider, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts that the Provider may directly have with any upstream provider entities. Included as part of **Appendix A** to this

Robocall Mitigation Plan document is a list of the Provider's current, immediate "Upstream Provider(s)" along with contact information for each.

## **VII. ONGOING ROBOCALL MITIGATION PRACTICES**

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator. TransNexus' ClearIP product generates reports based upon suspicious call pattern activities and use of unconventional Calling Party Number formats. Its database contains Calling Party Numbers of known rogue actors and instructs our switch to block those calls in real-time.

## **VIII. THIRD-PARTY CALL ANALYTICS**

The Provider also uses third-party call analytics to further assist and prevent the origination of illegal robocalls on its network. TransNexus' ClearIP product produces daily reports of originating traffic that could be potential RoboCalls. Included in **Appendix A** is the name of the vendor(s) used along with a description of the call analytics system(s) used to identify and block illegal robocall traffic.

### **ADDITIONAL CERTIFICATION RELATED INFORMATION**

The Provider certifies that it has not, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing relating to claims of transmitting,

encouraging, assisting or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

The Provider also certifies that it has not been prohibited by the Commission from filing in the Robocall Mitigation Database and that none of its prior certifications submitted in the Robocall Mitigation Database have been removed by Commission action.

Further, to assist the Commission in its ability to review and evaluate all Robocall Mitigation Database filings, The Champaign Telephone Company provides the following information identifying its principals:

**Company Officers:**

Timothy L. Bolander, President/GM

Tiffany M. Ebersold, CFO

**Board of Directors:**

Dwight D. Kent

Roy A. Doss

Timothy L. Bolander

Tiffany M. Ebersold

Cynthia J. Huffman

The Champaign Telephone Company does not have shareholders/owners with 50% or greater ownership in the company.

## **Appendix A**

### **Traceback Request Single Point of Contact:**

Name: Roger Barnhart

Title: Operations Manager

Phone Number: 937-653-2233

Email Address: roger@ctcommunications.com

### **Upstream Provider Information:**

Name of Upstream Provider: Sinch (Inteliquent)

Nature of Business: ProviderLD origination and termination provider

Network Location of Upstream Provider: Chicago IL

Name of contact: Client Services

Phone Number: 470-300-8394

Email Address ClientServices@inteliquent.com

### **Call Analytics Vendor Name and Description of System:**

Name of Vendor: TransNexus

Description of the call analytics system: ClearIP uses SIP Analytics to perform dynamic fraud analysis before call setup. It automatically learns the call traffic patterns for each individual subscriber/trunk and destination. It can detect and prevent fraud attacks in milliseconds while legitimate calls continue uninterrupted. It's the fastest, easiest, most precise way available to detect and prevent telecom fraud.

Call analytics purchased from the vendor determine if originating calls should be blocked. If the telephone number appears on a Do-not-call list or otherwise is an unallocated, unused, or invalid number, the call will be determined to be fraudulent and needs to be blocked. Vendor may also use advanced fraud detection which enables behavior analysis and tracking of abnormal and unexpected calling patterns to detect high volume robocalling, spoofing, and suspicious call activity.