



Common Knowledge Technology, Inc.
Robocall Mitigation Certification and Plan

This Robocall Mitigation Plan is submitted by Common Knowledge Technology, Inc. (CKT) pursuant to the provisions of § 64.6305 of the Federal Communications Commission's (FCC) rules, which require all voice service providers to establish a robocall mitigation plan. CKT provides voice services using 3CX for call management with Bandwidth.com as our wholesale voice provider.

STIR-SHAKEN IMPLEMENTATION STATUS

Common Knowledge Technology, Inc. is a voice provider who has implemented STIR/SHAKEN by contracting with our underlying voice provider, Bandwidth.com (Bandwidth), to also act as our third-party hosted signing service. All calls are signed.

ENFORCEMENT

All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan.

CKT has not received any enforcement actions.

CKT and/or any entity for which the filing entity shares common ownership, management, directors, or control have never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing.

TRACEBACK

CKT commits to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any robocallers that use our service to originate unlawful robocalls. CKT will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our service to carry, process, or originate robocalls.



IDENTIFYING INFORMATION

- Business name(s): Common Knowledge Technology, Inc.
- Primary address of the provider: 44 Inverness Dr E, Suite C; Englewood, CO 80112
- CKT is not a foreign voice service provider.
- OCN: N/A
- Principal: Peter Horewitch, President
- Robocall Mitigation Issues Contact

Benjamin Bryson

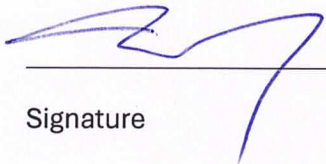
Senior Consultant

Phone Department

bbryson@ck-tek.com

720-863-1990 x 8050

I, Jeremy Palay, Vice President for Common Knowledge Technology, Inc. submit this certification on behalf of CKT, which has implemented the STIR/SHAKEN authentication framework as indicated in the Robocall Mitigation Database. Pursuant to section 1.16 of the FCC's rules, I certify, under penalty of perjury, that the information and statements contained herein are true and correct to the best of my knowledge and belief.



Signature

March 6, 2022
Date



Robocall Mitigation Plan

CKT views these policies and procedures as constituting reasonable steps to avoid the origination of illegal robocalls on our network. All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan.

As a reseller, CKT relies on Bandwidth's call analytics to monitor call traffic.

In its RMD filing, Bandwidth states that it:

- has a team of operational experts who have implemented technical and operational processes and procedures to monitor, detect and analyze the use of its services and traffic on our network that helps to determine when illegal and inappropriate robocalling activity may be occurring;
- has developed and deployed a "Call Blocking Tool" that incorporates industry best practices into its core network to identify and block invalid, unallocated and otherwise obviously illegal telephone numbers;
- follows established processes and procedures to notify upstream customers of the problematic traffic and request that they take immediate corrective actions to prevent recurrence of the illegal calls;
- consistently analyzes its call detail records to identify problematic call patterns and their sources.

Additionally, CKT has procedures in place to confirm the calling customer's right to use a telephone number. CKT's customers are permitted to use a telephone number as their caller identity if a number is directly managed by CKT and/or obtained by CKT 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, CKT screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber.

Know-Your-Customer Processes

CKT will use best practices in vetting the identity of all of its voice service subscribers. The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, CKT looks to confirm the identity of customers by 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. CKT vets subscribers during the process of provisioning customer requested services (for example in



appropriately sizing the facilities to their claimed intended use), executing CKT's required service agreements, and granting the customer the right to use telephone resources. Certain users, such as larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls. Such customers, at CKT's discretion, may be subject to an additional review, including a more stringent background check and a site visit.

CKT:

- Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of CKT provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and CKT reserves the right within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.
- Has established a process of routinely monitoring 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 CKT identifies activity or a pattern consistent with illegal robocalls, the customer will be contacted within twenty-four hours for further investigation and possible action regarding their subscribed voice service.

Know-Your-Upstream Providers

CKT relies on Bandwidth's Know-Your-Upstream Provider processes.

Traceback

CKT will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.