

Essensys, Inc. (“essensys”) submits this updated Robocall Mitigation Policy to provide additional details on the steps we are taking to avoid the origination of robocall traffic on its network.

essensys had previously not implemented STIR/SHAKEN due to eligibility for the small voice service provider extension to the implementation deadline (47 C.F.R. §64.6304(a)). essensys has now fully implemented STIR/SHAKEN throughout its network. All calls originating on essensys’ network are subject to a robocall mitigation program consistent with Section 63.6405 of the Commission’s rules.

1. General Prohibition of Robocalling

essensys customers are subject to the essensys terms of service (‘TOS’), including the End User Policy (‘EUP’), which must be affirmatively accepted prior to being offered service. Section C of the essensys EUP covers restrictions placed on our voice services and specifically includes language to restrict users from using essensys voice services: (i) to operate an automated call centre service; and (ii) for any illegal purpose or in any illegal manner. essensys retains the right to terminate access to voice service if users breach any restriction of the EUP, including using the service for an illegal purpose such as a robocalling.

2. Robocall Mitigation

essensys takes a number of reasonable steps to avoid originating illegal robocall traffic as part of its robocall mitigation policy, which it believes can reasonably be expected to significantly reduce the origination of illegal robocalls. essensys also collects and maintains accurate call detail record information that may be accessed when responding to traceback requests. essensys will promptly and diligently investigate any reported robocalls originating on its network and will take appropriate action (up to and including account suspension and termination) as authorized under its TOS and EUP.

A. Traffic Monitoring

essensys conducts ongoing, real time, monitoring of subscriber voice traffic patterns to identify suspicious traffic consistent with illegal robocalling. This monitoring is performed in-house using a combination of our own software and third party products

running on our servers. This includes, but is not limited to analytics related to the following:

- Call attempts per second (“CAPS”). Monitored to detect a suspicious increase in outbound calls. We have identified specific thresholds that would indicate unusual call traffic and configured alerts when these thresholds are exceeded.
- User Agents. Identifying what type of device is making the calls and flagging suspicious user devices. We dynamically build a per user list of acceptable devices for calls and flag calls made by other device types. Additionally we have a list of device types that are always considered suspicious.
- Time of Day. Flagging calls made at suspicious times of day. We dynamically build a time of day model per user and flag large numbers of calls outside those times.
- Destinations. Flagging suspicious destination patterns. We have a static list of high fraud destinations that generate alerts when calls are made to them.
- Registration attempts. Flagging suspicious attempts to register or access the essensys voice platform in order to prevent unauthorised users from registering with our voice platform. We have identified a specific registration rate that corresponds to normal traffic. If the total number of registrations attempts goes beyond that threshold an alert is generated and an engineer investigates. Once a certain number of failed log-in attempts occurs, the account may be permanently locked out and can only be cleared after an investigation is conducted by an essensys engineer.

Suspicious traffic is identified to our engineers for further investigation as to whether illegal behaviour is occurring. Should it be determined that illegal robocalling is occurring, essensys will take appropriate action to address such behaviors.

B. Restricted Network Access

essensys voice services are exclusively provided to flexible workspaces where we are also the service provider responsible for managing the network and internet access. Flexible workspaces are office spaces where the landlord provides a majority of the amenities, such as the network infrastructure and voice services. As such, we are able to effectively control and restrict access to our voice platform at the IP network level. For instance, default SIP ports are only accessible from IP addresses of known essensys-managed firewalls, which must be explicitly allowed in order to connect a SIP endpoint. This restricts the potential for a malicious third party to access our voice services and initiate illegal robocalls.

C. Customer Restrictions

essensys voice customers are all flexible workspaces where we are also managing the local area network as well as the internet connectivity. This ensures that we are only deploying physical handsets or analogue lines to known locations. We verify the business address as part of connecting the site to our network and perform know your customer checks on our partners, who are the flexible workspace operators. Our partners then perform additional know your customer checks on the end users, who will be based out of their buildings. Each subscriber is understood to be a typical office user and appropriate call limits are implemented so that any one line can only generate a limited number of concurrent calls. Caller ID presentation is restricted to only allow users to set their Caller ID number to phone numbers allocated to their company. Essensys also does not provide autodialing features to its customers.

3. Traceback Cooperation

essensys is committed to respond fully and in a timely manner 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 robcallers that use its service to originate calls. For example, in preparation for this commitment, essensys has ensured sufficient company capacity and protocols to provide prompt and complete responses to traceback requests. We have a group email responsible for receiving requests that is distributed to all appropriate employees. We have a designated on-call employee so that we can cover this 24/7/365.

Upon receipt of a traceback request, essensys endeavors to promptly respond within the timeframes expected by the FCC and the Industry Traceback Group.

This Robocall Mitigation Policy describes the measures that essensys has implemented to detect and prevent illegal robocalls as of the date of filing. essensys will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described, and take appropriate actions as necessary.

4. Validating Upstream Providers

We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate or transit to other providers.

We confirm that the upstream provider has a certification in the Robocall Mitigation Database. We will not accept voice traffic from an unregistered provider.

We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic.

We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider. We use this information to understand whether we will be obligated to authenticate unsigned traffic that we receive from them.

Our contractual provisions with upstream providers prohibit them from sending us illegal robocalls. If we find that an upstream provider is sending us suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

5. STIR/SHAKEN

We have registered with the STI-PA using OCN 658K. We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.