

Total Electronics Contracting, Inc. Robocall Mitigation Compliance with TRACED Act

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

We are a reseller of phone service to end users, thus all calls into or out from our end users are subject to the policies of the 2 upstream providers from whom we resell service.

Mitigation Program

In coordination with the ITG, our upstream providers perform Do Not Originate (“DNO”) based upon a reasonable DNO list, which may include blocking of government and other impersonation calls. They update their tools to keep ahead of and detect invalid phone number formats, area codes and unassigned number blocks. They also utilize internal data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

We use the following affirmative, effective measures to further prevent the origination or transit of illegal robocalls:

Know Your Customer

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

All new customers are required to fill out a new customer form which includes physical address, personnel names of leadership staff, alternate phone numbers, and billing information.

Know Your Upstream Provider

We have a direct relationship with 2 upstream providers, Coredial(Skyswitch) and ESI. Their contact information is listed below. We rely on them to know their upstream providers.

This is ESI’s plan:

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.

This is Coredial's plan:

The Company has an Upstream Provider Policy required to access the Company's networks to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. If the customer is a Voice Service Provider, the Company confirms that the provider is appropriately listed in the FCC's RMD and has not been delisted pursuant to an enforcement action before accepting traffic from the provider.

Traceback

We commit to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. We shall cooperate with these groups to investigate and stop any illegal robocallers from using our service to carry or process illegal calls. When notified by the FCC's Enforcement Bureau, we shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis (unless our investigation determines that the traffic is not illegal) when we receive actual written notice of such traffic from the Enforcement Bureau. If we determine that the identified traffic is not illegal, we shall provide the Enforcement Bureau with an explanation as to why we reasonably concluded that the identified traffic is not illegal, and what steps it took to reach that conclusion.

Analytics systems to identify and block illegal traffic

Calls processed through ESI use this set of analytics:

1. We use call analytics software provided by TransNexus (a third-party vendor) to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.
2. We perform the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. We immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

Calls processed through Coredial use this set of analytics (no third-party vendors are listed):

1. Monitoring the network to identify suspicious traffic patterns.
2. Limiting customers' capacity via call per second and/or concurrent session limits.
3. Regularly checking call patterns for possible abusive traffic.
4. All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. We severely limit the capabilities of new accounts until these appropriate processes are complete.

STIR/SHAKEN

Our upstream provider ESI has registered with the STI-PA using OCN 983J. They have their own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that they use

when authenticating calls we originate. They have implemented a STIR/SHAKEN solution supplied by TransNexus.

Our upstream provider CoreDial has fully implemented STIR/SHAKEN. All calls that we originate are compliant with Sections 64.6301(a)(1) and (2) of the Commission's rules

Total Electronics Contracting, Inc. has three upstream providers from which it sends and receives voice traffic:

1. PayG LLC dba SkySwitch
Arborcrest 1, 751 Arbor Way
Suite 150
Blue Bell, PA 19422
Phone: 747.777.8100
Email: support@skyswitch.com
2. CoreDial LLC
Arborcrest 1, 751 Arbor Way
Suite 150
Blue Bell, PA 19422
Phone: 215.297.4400
Email: cdsupport@skyswitch.com
2. Estech Systems, Inc (ESI)
3701 E. Plano Parkway,
Ste. 300
Plano, TX 75074-1819
Phone: 972.422.9700

We reserve the right to refuse traffic from any party at any time where robocalling or use of originating numbers that are not valid or they are not authorized to use has occurred or is suspected. We are able to block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number transiting our networks.