

**Upper Peninsula Telephone Company and Michigan Central Broadband Company
Policy and Procedure for Robocall Mitigation Plan
As of February 28, 2026**

Upper Peninsula Telephone Company and Michigan Central Broadband Company have implemented Metaswitch's Call Guardian for Robo Mitigation and Transnexus software for a full Stir/shaken compliance platform.

Robocall Mitigation Plan

Know Your Customer

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

STIR/SHAKEN

We sign outbound off network traffic calls with STIR SHAKEN certificates.

Robocall Mitigation Program

We use software provided by TransNexus to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts us if we originate any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. We immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

1. Takes steps to mitigate illegal traffic when notified by the Enforcement Bureau.
2. Takes affirmative, effective measures to prevent new and existing customers from making originating illegal robocalls.
3. The provision of voice service by the company assumes that only legitimate calls will be originated or terminated. It is illegal when a caller transmits misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongly obtain anything of value. The company will cooperate with

the Federal Communications Commission and law enforcement to provide them with information necessary to mitigate illegal traffic.

4. Amends contracts, as deemed appropriate, to prohibit illegal mass calling with the right to disconnect service.

5. Every effort is made, to the best of our abilities, to block a call if it is highly likely to be illegitimate such as:

a. The originating telephone number should be network-blocked because it shows up on a Do Not Originate list or is an unallocated, unused, or invalid number.

b. Because reasonable analytics indicated the call is likely malicious in intent. For example, a significant change in a business' originating traffic patterns to suddenly become high volume, very short duration calls might indicate they have been hacked.

6. Upper Peninsula Telephone and Michigan Central Broadband are implementing Metaswitch's Call Guardian Authentication Hub.

- a. Metaswitch utilizes Call Guardian Authentication Hub to simplify signing of inter-carrier calls by automatically authenticating and verifying calls and applying the appropriate call validation treatment.
- b. Call Guardian analyzes network data, along with other factors from numerous data sources including crowd-sourced feedback, to arrive at its scores and categories.
- c. Call Guardian's algorithm examines calling history, volume, and pattern irregularities.
- d. All TNs are scored positively or negatively. Negative TNs are scored from -4 to -1, from most likely to be a caller perpetrating a scam, to caller most likely to be a benign, but nuisance, telemarketer.
- e. Operators have the option to block some scores and warn about others. Flexibility and certainty increase the likelihood they will block the most problematic calls.
- f. Bad actor TNs are categorized as: Robocaller, Spammer, Spoofer, and Scammer.
- g. Provides traceback and industry wide dispute resolution.
- h. Customer Care can resolve disputes by answering key questions as to why a customer's number is marked as Spam.
- i. Outbound calls are sent to Call Guardian for analysis, works with SIP and TDM, calls are not blocked, in contrast with inbound traffic.
- j. Results are visible in portal enabling Operators to see patterns and drill down, taking action where needed.

The Call Guardian Authentication Hub (CGAH) is a managed and hosted end-to-end solution that analyzes real-time call events with authentication to determine call treatment. The integrated solution is powered by TNS and Metaswitch enabling providers to meet TRACED act requirements and deliver an improved subscriber user experience.