

Robocall Mitigation Plan

Know Your Customer:

At NHC, best practices for vetting caller identity, as outlined by the NANC Call Authentication Trust Anchor Working Group¹, are followed. This includes the collection of end-user name, billing address, service address, and credit history (to the extent permitted by applicable law). For business customers, NHC also collects information such as the nature of the customer's business to confirm that the customer is engaged in legitimate business activity. We recognize the significance of verifying the authenticity of our customers to mitigate the risk of involvement with illegal robocall activities.

Terms of Service and Acceptable Use Policies:

In addition to Master Service Agreements and Service Orders, NHC maintains Terms of Service and an Acceptable Use Policy that apply to the use of all service provided by NHC to its customers. Both policies contain provisions designed to mitigate illegal robocalls.

The Terms of Service prohibit the use of the service in any manner that violates Federal, State, or Local laws and reserves the right for NHC to discontinue service without notice in the event of any such unlawful use. Under the Terms of Service, the use of NHC's services for any unlawful purpose or for any purpose other than that for which the service is intended constitutes a default that permits NHC to terminate the service for cause. The Terms of Service also identify the customer's provision of inaccurate, false, or otherwise misleading information in an application for service as an event of default triggering termination for cause. By accepting the Terms of Service, customers represent and warrant that their use of the service will comply and conform with the Acceptable Use Policy and all applicable laws and regulatory requirements.

Similar to the Terms of Service, the Acceptable Use Policy prohibits the use of NHC's IP-related services for unlawful purposes (as determined in NHC's sole discretion) and prohibits the use of the services for the transmission of bulk e-mails and spam.⁶ Violation of the Acceptable Use Policy may result in suspension or termination of the services in NHC's sole discretion.

Traceback Response:

New Horizon Communications is dedicated to a prompt and comprehensive response to all traceback requests from regulatory bodies such as the FCC, law enforcement agencies, and industry traceback consortiums. We commit to collaborating fully in investigations to identify and cease the activities of illegal robocalls using our services to originate, carry, or process illegal robocalls. Our response time to traceback requests is set at a maximum of 24 hours, and NHC commits to respond to all traceback requests within the 24 hour response time.

THE Communications STACK Provider™

**Robocall Mitigation Program:**

NHC has fully implemented the STIR/SHAKEN Caller ID Authentication Framework. As part of our proactive approach to mitigating robocall threats, we also employ software provided by TNSI, known as Call Guardian.⁷ This software actively monitors our voice traffic, offering detailed reporting to identify and address suspected illegal robocalls promptly.

The software alerts us to calls where the calling number is invalid, unallocated, on a Do Not Originate list, listed in the FCC consumer complaint database, or has a poor reputation. Immediate investigation follows any identified calls to determine if the caller was attempting to originate unlawful robocalls. In cases where unlawful robocall attempts are confirmed, appropriate action is taken, including issuing warnings or terminating services as necessary.

In addition to its customer vetting procedures consistent with the NANC Call Authentication Trust Anchor Working Group, NHC conducts investigations into new customers seeking access to high-volume origination services. This diligent vetting process allows us to identify and address any potential risks before onboarding new clients.

We are committed to taking reasonable and effective steps to ensure that our network is not exploited for the transmission or processing of a high volume of illegal traffic. This involves exercising due diligence before accepting traffic from upstream providers.

NHC's Upstream providers Level 3, Bandwidth, SINCH all deploy their own RMP