



No customer should ever be treated like a number

ipSBS Managed Services, LLC dba HostMyCalls & HostMy Robocall Mitigation Plan

Introduction

HostMyCalls has less than 100,000 subscribers and provides hosted voice/PBX services to businesses based in the United States. HostMyCalls does not act as an intermediate gateway, does not sell wholesale services, does not provide lead generation services, traffic aggregation, or bulk call origination services, and does not provide service to international customers unless the business is headquartered in the United States.

Our Primary Place of Business:

3035 Sutherland Ave
Knoxville, TN 37919

Risk Assessment

HostMyCalls (HMC) is a voice service provider offering hosted voice and PBX services primarily to small and mid-sized U.S.-based businesses. Endpoint connections to HMC's network are tightly controlled by HMC support and engineering staff. HMC does not provide wholesale origination services, does not act as an intermediate gateway, and does not permit customers to originate calls using unverified Caller IDs. Customers are limited to verified numbers provisioned by HMC and are subject to simultaneous call thresholds and automated monitoring for abnormal activity. Based on these controls, its flat-rate pricing model, and the nature of its business customer base, HMC assesses its network as presenting a low risk of originating illegal robocalls.

Know Your Customer - Establishing New Service

HMC establishes new service through a contractual agreement process that follows the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>). HMC contracts stipulate that all users of its voice services comply with applicable laws prohibiting illegal robocalling. Those same contracts allow for blocking and/or termination of services for users that breached such provisions. During the agreement process, HMC collects physical business location, the name of an officer of the company, Federal Employer Identification Number (as necessary) and contact person (if different).

All services are provisioned on designated end-point hardware, soft-clients supplied by HMC or user authentication. Whether the service is supplied through hardware, software or 3rd party telephone systems, each customer may only use Caller IDs from a specific list created by the HMC provisioning team. The numbers on the Caller ID list must be ported by HMC on behalf of the customer and verified



No customer should ever be treated like a number

by the customer's invoice supplied by another carrier. No other Caller IDs are allowed, and customers may not Spoof a Caller ID.

HMC has policies in place that define the circumstances by which it will deny, suspend or terminate service to a customer. Most services are installed initially by a representative of HMC at the customer's location(s).

Preventing New and Renewing Customers from Originating Illegal Calls During Service

As mentioned previously, customers may only use numbers from a list where their ownership has been established preventing HMC customers from illegally spoofing the numbers of others. Customers have access to call filters and blocking mechanisms that allow them to block calls from unwanted numbers.

HMC sells its services on a flat-rate basis for calls within the continental United States. Each customer account consists of one or more designated "Users," and outbound call activity is subject to concurrent call thresholds and monitoring controls. Because HMC does not offer usage-based wholesale origination and does not provide bulk traffic services, significant automated outbound call activity is not consistent with HMC's service model.

Customers may not connect automated outbound dialing software to HMC services without prior written approval from HMC engineering. Requests to use automated outbound dialing applications are reviewed for:

- the nature and purpose of the calling activity,
- expected call volumes and patterns,
- compliance with applicable federal and state laws, including TCPA requirements, and
- alignment with the customer's subscribed service capacity.
-

Approved applications are provisioned with appropriate call thresholds and are subject to ongoing monitoring for abnormal or excessive traffic patterns. HMC reserves the right to suspend or terminate automated outbound dialing privileges if traffic patterns indicate potential unlawful activity or violation of HMC's service agreement.

Customers approved for automated outbound dialing are reminded of their legal obligations to comply with federal law, FCC regulations, and all applicable consumer protection requirements.

Additional safeguards are placed on all customers that limit simultaneous calls to their subscribed services and flag total voice call minutes that exceed their subscribed activity.

HMC runs daily automated reports looking for suspicious robocalling activity generated from HMC customers. Suspicious activity is escalated to engineering and compliance staff for manual review.



No customer should ever be treated like a number

HMC maintains a database of all calls on its network and includes the Caller ID of the originator and public IP addresses of all parties. The HMC database will be used to traceback any suspicious activity and to cooperate with law enforcement.

After Service Has Been Used for Illegal Activity

HMC retains call detail records, including Caller ID and source IP information, for a minimum of 12 months to support traceback investigations. HMC has a designated email address to receive traceback requests: traceback@hostmycalls.com.

HMC commits to respond within 24 hours to all traceback requests from the FCC, law enforcement and the industry traceback consortium. HMC further commits to cooperate with such entities in investigating and stopping any illegal robocallers from using its services to originate calls.

Upon receiving a Traceback request, HMC will use its monitoring tools to:

- Investigate and identify the source of the traffic
- If originated within HMC network, verify the Caller ID number sent to a receiving party matches authorized Caller ID's for the customer
- If abuse is found, terminate the party's ability to originate calls

Know Your Upstream Provider

HMC maintains 2 relationships connecting its network to upstream providers and has verified their entries in the RMD.

Bandwidth, Inc.
2230 Bandmate Way, Raleigh, NC 27607
(855) 864-7776
tacsupport@bandwidth.com
RMD0002564

Sangoma U.S., Inc.
301 N Cattlemen Rd, Ste 300, Sarasota, Florida 34232
(941) 960-8284
legal@sangoma.com
RMD0002434

HMC has reviewed these carriers entries and their Robocall Mitigation Plans (RMP).

STIR/SHAKEN



No customer should ever be treated like a number

HMC has fully implemented STIR/SHAKEN using Sansay's Number-Lookup for STIR/SHAKEN (NSS). HMC signs calls originating from authenticated customers using full A-level attestation when it has a direct authenticated relationship with the customer and has verified the right to use the calling number. Calls that do not meet full attestation criteria are appropriately downgraded in accordance with ATIS standards.

Addendum

HMC was notified on FCC Order DA 24-1235 made on December 10, 2024 that it needed to cure deficient Robocall Mitigation Database filings. HMC subsequently corrected the deficiency. HMC certifies that it is not, nor has it, been prohibited from filing in the Robocall Mitigation Database and at no other time (other than mentioned above) in the past 2 years has HMC been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation due to (i) transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls; or (ii) a deficient Robocall Mitigation Database certification or mitigation program and description.