

HOTWIRE COMMUNICATIONS, LTD.

Federal Communications Commission
Robocall Mitigation Plan

Last Updated: March 2026

Hotwire Communications, Ltd.
Robocall Mitigation Plan

Table of Contents

I.	Robocall Mitigation Plan Introduction.....	3
I.A	Company Summary	3
I.B	STIR/SHAKEN Status — Hosted Signing for Outbound Calls; No Extension	4
II.	Robocall Mitigation Plan.....	4
II.A	Customer Onboarding and Know Your Customer Protocols	4
II.B	Terms and Conditions of Agreements	7
II.C	Analyzing and Monitoring Network Traffic	9
II.D	Participation in the Industry Traceback Group (ITG).....	10
II.E	Investigating and Mitigating Suspicious Calling Patterns	11
II.F	Regulatory History and Enforcement Matters	12
II.G	Designated Robocall Mitigation and Traceback Contact	12
II.H	Plan Updates and Future Commitments	12
	Exhibit A – Company Information	14

I. Robocall Mitigation Plan Introduction

This Robocall Mitigation Plan describes the specific reasonable steps that Hotwire Communications, Ltd., on behalf of itself and its subsidiaries and affiliates (see Exhibit A) (collectively, “Hotwire” or the “Company”), takes to prevent unlawful robocalls from originating on its voice network and to support Hotwire’s Robocall Mitigation Database (“RMD”) certification. This Plan applies to all of Hotwire’s calling platforms.

Guiding frameworks. Hotwire’s robocall mitigation program is informed by government and industry guidance, including the 2019 State Attorneys General anti-robocall principles for voice service providers and the USTelecom Industry Traceback Group (“ITG”) Policies and Procedures. The controls described in this Plan—including customer due diligence for Business/Enterprise¹ customers (Section II.A), network monitoring and analytics (Section II.C), investigation and mitigation workflows (Section II.E), and cooperation with traceback requests (Section II.D)—are designed to align with these frameworks and with Hotwire’s FCC obligations.

I.A Company Summary

Hotwire is a privately owned company headquartered in Fort Lauderdale, Florida, with its principal place of business at 2100 West Cypress Creek Road, Fort Lauderdale, FL 33309. The Company was founded in 2000 and provides broadband, video, and voice services over a fiber-optic network it owns and operates. Hotwire offers these services in Arizona, California, Florida, Georgia, Nevada, New Jersey, North Carolina, Pennsylvania, South Carolina, Tennessee, and Texas. Its Business/Enterprise customers include community-living communities, businesses, hotels and resorts, student housing environments, and senior living facilities.

In the Company’s service territories described above, Hotwire provides IP-only, facilities-based Voice over Internet Protocol (“VoIP”) originating and terminating service to residential and Business/Enterprise end users. Hotwire exchanges traffic with an upstream voice provider for call completion and, where applicable, Caller ID authentication functions. One of these upstream providers also supports telephone number inventory management and local number portability (LNP) for ports to Hotwire.

Hotwire is not a foreign voice service provider; it does not operate as a gateway provider introducing foreign-originated traffic into the U.S. public switched telephone network (“PSTN”), does not provide intermediate transit services for unaffiliated carriers, and does not hold itself

¹ For purposes of this Plan, “Business/Enterprise” refers to Hotwire’s non-residential customer category, including business, commercial, and enterprise customers. References to specific agreements, forms, or tariffs use the applicable document’s formal title.

out as providing wholesale voice carriage or Session Initiation Protocol (“SIP”) termination services for third-party voice service providers.

I.B STIR/SHAKEN Status — Hosted Signing for Outbound Calls; No Extension

Hotwire is an end-user voice service provider with a STIR/SHAKEN implementation obligation, and this Plan describes Hotwire’s STIR/SHAKEN processes and controls applicable to SIP calling and provider interconnection, including hosted signing as described below and verification of inbound authentication information as described in Section II.C.

Hotwire authenticates caller identification information for calls originated on its network, including where such calls are exchanged with other voice service providers, using a hosted signing (third-party authentication) arrangement. In this model, Hotwire obtains and maintains its own Service Provider Code (“SPC”) token and Secure Telephone Identity (“STI”) certificate(s) and establishes Hotwire’s call signing / attestation policy. Hotwire determines the appropriate attestation level for calls originated by Hotwire customers. Hotwire’s upstream signing partner performs the technical function of applying the SHAKEN signature on Hotwire’s behalf using Hotwire’s STI certificate(s) and Hotwire’s signing/attestation policy.

Information collected through Hotwire’s Business/Enterprise onboarding process (including customer identity/business validation and number authorization documentation, as applicable) is used to support Hotwire’s call authentication attestation policy for outbound calling.

Hotwire maintains a memorialized written agreement governing any hosted signing arrangement that specifies the tasks performed by the third-party signer and confirms that (i) Hotwire makes attestation-level decisions for calls signed pursuant to the agreement and (ii) calls are signed using Hotwire’s STI certificate(s) (not a third party’s certificate).

Hotwire operates a fully IP-based network and does not rely on non-IP technology (e.g., Time Division Multiplexing or TDM) that cannot support STIR/SHAKEN. As such, Hotwire claims no extensions under 47 C.F.R. § 64.6304.

II. Robocall Mitigation Plan

II.A Customer Onboarding and Know Your Customer Protocols

Hotwire applies a risk-based onboarding program for voice services, with controls scaled to the customer segment and the customer’s anticipated calling activity. The subsections below describe Hotwire’s customer due diligence controls for Business/Enterprise customers, and its upstream-provider verification controls.

Business/Enterprise Customers. Hotwire follows Know Your Customer (“KYC”) protocols when onboarding new Business/Enterprise voice customers. As a baseline requirement, all new such customers must complete Hotwire’s Business Voice Service Use Questionnaire (Short Form), which captures core customer identity and contact attributes (legal name and doing business as (“DBA”) (if any), street address (including city/state/ZIP), business industry, website URL, Federal Employer Identification Number (“FEIN”)/Tax ID (as applicable), Hotwire account/customer ID (if known), and designated primary and traceback/robocall mitigation contacts (including name/title, email, and phone)). The Short Form also captures service context (service type and estimated number of lines/channels) and includes structured compliance screening to understand the customer’s intended calling practices, including: whether the customer will originate outbound calls; whether outbound calling is expected to be high-volume; whether the customer is a reseller or voice service provider, including traffic resale or origination on behalf of third parties; use of autodialing systems; use of prerecorded or artificial voice messages (including text-to-speech/AI-generated voice); campaign-based marketing/lead-generation/fundraising calling; use of third-party lead/list sources; and requests for custom caller ID using telephone numbers not assigned by Hotwire.

As a baseline onboarding control applied to new Business/Enterprise voice customers (regardless of the customer’s outbound calling profile), Hotwire reviews the customer’s onboarding and billing information as it is entered into Hotwire’s systems to confirm the account-setup information is complete, internally consistent, and facially plausible, and, where applicable, compares that information to Hotwire’s internal records associated with the customer identity, service address, or an existing Hotwire relationship, to identify and flag issues appropriate for follow-up. These onboarding controls support robocall mitigation by deterring activation of fraudulent or non-credible accounts used for unlawful calling activity and strengthening customer accountability through verified customer and billing information.

Customers whose Short Form responses indicate elevated robocall risk indicators (for example, high-volume outbound calling, reseller/voice service provider use cases, autodialer use, prerecorded/artificial voice, campaign/list-based outbound calling, third-party lead sources, and/or requests to present non-Hotwire caller ID) are required to complete Hotwire’s Business Voice Services Compliance & Caller ID Authorization Form (Long Form) as part of enhanced onboarding due diligence. The Long Form collects additional information to validate identity and calling profile, including: additional business verification attributes (date and jurisdiction of formation); confirmation of end-user vs. reseller/voice service provider status (and, where applicable, FCC 499 Filer ID and FCC Robocall Mitigation Database (RMD) ID); detailed outbound traffic profile information (e.g., estimated volume, concurrency, time-of-day patterns, duration, and monthly minutes); the nature and audience of outbound calls (e.g., informational/transactional, healthcare-related, Fair Debt Collection Practices Act (“FDCPA”)-regulated debt collection, other lawful purposes; and whether calls are directed to existing customers, prior customers, or third-party leads/prospects); designated compliance contacts (including traceback/robocall mitigation and emergency compliance contacts, including name/title, email, and direct phone); and expanded confirmations regarding autodialer use and

prerecorded/artificial voice calling (including platform/vendor details when applicable and whether such calls are directed to wireless numbers and/or residential landlines).

Where a customer requests custom caller ID using non-Hotwire telephone numbers, the Long Form also captures the specific telephone numbers requested, the ownership/source of each number, and supporting documentation (e.g., recent carrier invoice, carrier customer service record, and/or a letter of authorization, as appropriate). The Long Form additionally captures whether the customer requests Hotwire to consider applying Full (“A”) STIR/SHAKEN attestation for non-Hotwire numbers and acknowledges that telephone-number delegation (or similar) from the applicable carrier/numbering provider may be required.

Through these forms and any supporting documentation, Hotwire collects a standardized, documented customer profile sufficient to (i) identify the customer and responsible contacts; (ii) understand the customer’s intended outbound calling use cases and key risk indicators; (iii) document anticipated traffic characteristics (including volume); and (iv) validate Caller ID authorization (including any non-Hotwire numbers) using supporting documentation where appropriate. Hotwire uses this standardized customer profile and supporting documentation to support enforcement of the contractual restrictions in Section II.B and the monitoring and mitigation controls described in Sections II.C and II.E. In addition, Business/Enterprise customers certify that they will promptly notify Hotwire if the customer’s calling practices change in a way that would require updating any prior responses provided during onboarding.

Residential Customers. For its residential subscribers, Hotwire validates legal addresses through a third-party vendor before onboarding a customer (with an error code returned for insufficient information). As part of account setup, Hotwire reviews the customer’s onboarding and billing information to confirm its complete, internally consistent and facially plausible, including identity verification at service start and, where Hotwire has relevant internal history, internal record checks for prior outstanding balances, delinquent accounts, or other account-history indicators among new or renewing customers, to identify and flag issues appropriate for follow-up. These onboarding controls support robocall mitigation by reducing the likelihood that fraudulent or non-credible accounts are activated for unlawful calling activity and by strengthening customer accountability through verified customer and billing information.

Upstream Providers. Hotwire applies know-your-upstream-provider controls to its upstream provider relationships by periodically verifying each upstream provider’s status in the RMD, Intermediate Provider Registry (“IPR”), and (as applicable) Form 499 filings, as part of confirming required STIR/SHAKEN and robocall mitigation registrations and filings. If an upstream provider that is required to be listed in the RMD is not listed (or is delisted), Hotwire will refuse to accept traffic sent directly from that provider, consistent with 47 C.F.R. § 64.6305(g). Hotwire will take commercially reasonable steps to remediate such issues, which may include suspending acceptance of traffic from that source until the upstream provider’s required RMD status is restored. Hotwire periodically reviews its upstream-provider arrangements to help confirm that applicable agreements include commitments (i) not to transmit

**Hotwire Communications, Ltd.
Robocall Mitigation Plan**

improper traffic; (ii) to maintain required robocall mitigation registrations, (iii) to support Hotwire's twenty-four (24) hour traceback-response commitments; and (iv) to cooperate with the Commission, law enforcement, and the ITG in traceback-related investigations and efforts to investigate and stop suspected illegal robocallers, as appropriate and consistent with applicable requirements.

II.B Terms and Conditions of Agreements

Both Business/Enterprise and residential voice service customers of Hotwire are subject to service terms intended to support compliance with applicable law and to preserve Hotwire's ability to act in response to suspected misuse.

Business/Enterprise customers. For Business/Enterprise voice customers, baseline service terms are set forth in (i) Hotwire's standard Business/Enterprise service agreement(s) and (ii) Hotwire's Business Voice Service Use Questionnaire (Short Form). These baseline terms are supplemented, where triggered by the customer's responses to the Short Form, by (iii) the Compliance & Caller ID Authorization Form (Long Form) and, where applicable based on location/service, by (iv) location-specific tariff terms for tariffed intrastate services (e.g., Pennsylvania).

Standard Business/Enterprise agreement. Under Hotwire's standard Business/Enterprise service agreement, Business/Enterprise customers agree not to use the services, products, or any Hotwire facilities/equipment in any unlawful way or for any unlawful purpose; agree to defend, indemnify, and hold harmless Hotwire against damages/costs caused by customer misconduct (including sending or receiving illegal or improper content); and acknowledge and agree that Hotwire may suspend or terminate services for specified triggers, including (among other triggers) violation of Hotwire's posted policies and suspected or actual fraud, misrepresentation, or other violation of law.

Short Form commitments. By completing the Short Form, Business/Enterprise voice customers certify that the information provided is true, accurate, and complete; that they will not use Hotwire's voice services to originate illegal robocalls; and that they will comply with all applicable federal and state laws governing automated, prerecorded/artificial voice, and telemarketing telephone calls placed using Hotwire's voice services. Customers further certify that they will promptly notify Hotwire if their calling practices change in a way that would require updating prior responses, and that they will cooperate with reasonable traceback/robocall-mitigation inquiries, responding as promptly as practicable and, in any event, within twenty-four (24) hours of receipt. By completing the Short Form, customers also acknowledge and agree that Hotwire may require additional diligence (including completion of the Long Form and/or supporting documentation) before enabling outbound calling or custom caller ID features; and that providing false or misleading answers constitutes a material breach of the customer's service terms and may result in immediate suspension of outbound calling capabilities and/or other remedial action permitted under those terms.

Hotwire Communications, Ltd. Robocall Mitigation Plan

Long Form commitments. Where a customer is required to complete the Long Form (as triggered by the customer’s responses to the Short Form), the customer’s completion and signature of the Long Form constitute the customer’s representation, warranty, and agreement—as conditions to outbound calling enablement and related service configuration—that it will comply with “applicable legal, regulatory, and industry requirements,” including, as applicable, requirements referenced in the Long Form relating to the Telephone Consumer Protection Act (“TCPA”), the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”), and ITG processes. The customer’s completion and signature of the Long Form likewise constitute the customer’s acknowledgement and agreement (as applicable) to comply with the telemarketing/prerecorded-call requirements referenced in 47 C.F.R. § 64.1200, including call-volume limits, automated opt-out mechanisms, and company-specific do-not-call rules. The Long Form further includes an allowance for redaction/de-identification in connection with traceback/mitigation or emergency compliance inquiries where compelled by applicable privacy laws.

Non-Hotwire Caller ID. Where a customer requests custom outbound caller ID using telephone numbers not assigned by Hotwire, the customer’s completion and signature of the Long Form constitute the customer’s representation and warranty that it has the full legal right (ownership or explicit authorization) to use each such number as outbound caller ID, and that it will not knowingly cause misleading or inaccurate caller identification information to be transmitted with intent to defraud, cause harm, or wrongfully obtain anything of value (including as described in the Long Form’s Truth in Caller ID Act representation). The customer’s completion and signature of the Long Form likewise constitute the customer’s acknowledgement and agreement that, if inaccurate, unauthorized, or misleading caller ID information is provided, Hotwire may immediately disable use of such number and/or outbound calling pending remediation. Where the Long Form applies, the customer also acknowledges and agrees that Hotwire will not activate outbound origination or configure any non-Hotwire caller ID telephone numbers until the Long Form is fully completed, signed, and returned, and that Hotwire may suspend or discontinue outbound calling where warranted under the Long Form (including where information is false or calling activity violates the customer’s representations or applicable law).

Pennsylvania tariffed services. For customers receiving tariffed intrastate regulated telecommunications service in Pennsylvania, Hotwire’s applicable Pennsylvania Local Exchange Carrier (“LEC”) and/or Interexchange Carrier (“IXC”) tariffs state that the services shall not be used for any unlawful purpose or for any use for which the customer has not obtained all required governmental approvals, authorizations, licenses, consents, and permits; and that Hotwire may terminate service upon written notice to the customer if the customer is using the service in violation of the tariff or in violation of law.

Residential voice customers. Under Hotwire’s VoIP Consumer Service Agreement, residential customers agree not to use the services in any unlawful way or for any unlawful purpose, and customers acknowledge and agree that Hotwire may terminate or suspend service (at its sole discretion) for material noncompliance and other enumerated triggers, including

**Hotwire Communications, Ltd.
Robocall Mitigation Plan**

violation of any legal requirement and suspected or actual fraud or misrepresentation (or commercially reasonable suspicion thereof).

II.C Analyzing and Monitoring Network Traffic

Role-appropriate mitigation posture. Hotwire’s monitoring and mitigation controls are designed for its role as an originating and terminating provider and are supplemented, where applicable, by upstream-provider controls (including where upstream providers perform intermediate-path functions).

Monitoring program (automated analytics, alerting, and indicators). Hotwire continuously monitors voice traffic using an automated monitoring stack that performs real-time and near-real-time analysis of (i) call detail record (“CDR”) data and (ii) network-element reporting (e.g., Session Border Controller (“SBC”)/softswitch logs and associated dashboards). Hotwire also uses third-party analytics and reputation data to identify high-risk traffic. Hotwire supports this monitoring using tools including the TransNexus Real-Time Anti-Fraud platform and Sansay Session Border Controller service monitoring (including Real-Time Service Monitor (RSM) and Proactive Service Monitor (PSM)). As part of this monitoring program, Hotwire also reviews, as available, upstream-received traffic characteristics (such as short-duration call frequency and answer-seizure ratios).

These tools surface indicators such as unusual burst volumes and atypical calling distributions that may suggest unlawful robocalling. When defined thresholds or indicators are triggered, the monitoring stack generates alerts and/or tickets for operational review and response.

Complaints and inquiries as monitoring signals. Hotwire treats credible customer complaints, customer service inquiries, and other third-party reports (including traceback notifications and related communications; see Section II.D) as signals that inform operational triage and monitoring. Hotwire tracks and triages these reports through its customer support and compliance processes and uses them to refer calling patterns for additional review and to help identify suspicious traffic trends, including where the reported issue involves suspected caller ID spoofing using Hotwire-issued numbers or suspected misuse of a Hotwire customer’s outbound calling configuration. These reports may be received through Hotwire’s customer support channels (e.g., phone, live chat, and contact form) and are handled through Hotwire’s triage process for review consistent with this Plan, including escalation for investigation and mitigation where warranted.

Preventive call treatment controls (DNO/invalid-number blocking). In addition to the investigative/mitigation measures described in Section II.E, Hotwire maintains standing preventive call-treatment controls through its upstream-provider arrangement. These controls include upstream-provider blocking of calls associated with numbers identified on applicable industry Do Not Originate (DNO) lists (including the Industry Traceback Group DNO list),

where applicable under FCC DNO requirements and related rules. These controls use network-element enforcement and screening informed by DNO registries and call detail record (“CDR”) and network-element indicators, and may include real-time screening where implemented, to prevent origination and/or termination of traffic from such sources, consistent with applicable service terms (Section II.B).

Complementing these network-level capabilities, Hotwire provides subscriber-facing resources to help customers identify and reduce unwanted robocalls, including service resources describing available voice features and controls. Subscribers have access to caller identification and call management features such as caller ID/calling name retrieval and call-control features (e.g., Anonymous Call Rejection, Selective Call Rejection/Acceptance, and Do Not Disturb). Hotwire provides subscribers with a reasonable mechanism to manage available call treatment features, including via star codes and/or a subscriber portal (where available) and/or through Hotwire’s customer support channels.

Hotwire maintains a process to review and address credible reports of unexpected call treatment outcomes. This process includes intake through Hotwire’s customer support channels, internal review of relevant call signaling data, call detail records (“CDRs”), and available authentication/analytics telemetry, and reasonable corrective actions where warranted (including adjustment of call treatment parameters where operationally appropriate).

Hotwire does not impose a separate line-item charge for the subscriber-facing call management and call-control features described in the two immediately preceding paragraphs or for Hotwire’s process for reviewing and addressing credible reports of erroneous labeling or other unexpected call treatment outcomes.

Operational triage, escalation, and response coverage. Hotwire maintains a Network Operations Center (“NOC”) staffed with full-time employees to monitor Hotwire’s voice service operations on a continuous basis and to triage alerts and tickets generated by the monitoring stack. Where indicators warrant further review or action, the matter is escalated to the Hotwire Voice Engineering team for investigation and mitigation as described in Section II.E. When issues require engineering action, the Hotwire Voice Engineering team responds through an on-call/escalation process, including outside standard business hours, to address service impacts, fraud, and internal or external investigations.

II.D Participation in the Industry Traceback Group (ITG)

Hotwire is registered with the ITG, the industry traceback consortium, and responds within twenty-four (24) hours of receipt to all traceback requests from the FCC, law enforcement, and the ITG, with the twenty-four (24)-hour response period calculated in accordance with applicable FCC rules. Hotwire cooperates with such entities in investigating and stopping suspected illegal robocall traffic that uses Hotwire’s service, including by making relevant call information available as appropriate and consistent with applicable requirements.

Hotwire Communications, Ltd. Robocall Mitigation Plan

Where information necessary to complete a traceback response is maintained by Hotwire's upstream provider(s), Hotwire coordinates with such provider(s) to support timely and complete responses.

To support timely receipt and internal routing of traceback notifications, Hotwire lists multiple employees (including the designated employee identified in Section II.G) as recipients of traceback notices. Customer-designated traceback/robocall-mitigation contacts are collected through the Business/Enterprise onboarding process described in Section II.A, and customer cooperation and response-time commitments for traceback inquiries are addressed in the service terms described in Section II.B.

II.E Investigating and Mitigating Suspicious Calling Patterns

Investigation triggers and coordination. Hotwire initiates investigations upon (i) escalation from its monitoring and triage activities (Section II.C), including automated monitoring alerts, and credible complaints or inquiries; (ii) receipt of traceback requests or related notifications (Section II.D); and (iii) receipt of a Notice of Suspected Illegal Traffic from the FCC Enforcement Bureau. Following initiation, the team engages internal stakeholders and, as appropriate, legal counsel, assesses the traffic, and implements mitigation measures consistent with Hotwire's applicable service terms. Hotwire reviews relevant traffic characteristics and supporting data within its control (including call signaling data, CDRs, monitoring analytics, and other numbering/traffic-validity indicators, where relevant) and coordinates with the impacted subscriber as appropriate. Where the trigger is a Notice of Suspected Illegal Traffic, the team coordinates implementation of the mitigation measures in this section in a manner consistent with 47 C.F.R. § 64.1200(n)(2).

Mitigation measures. Mitigation measures include, as appropriate, (i) suspending or restricting outbound calling capabilities; (ii) disabling unauthorized caller ID configurations; (iii) blocking specific telephone numbers, call paths, or traffic signatures associated with suspected activity; and (iv) terminating service where warranted. Where appropriate, mitigation measures may also include applying or refining call-treatment controls described in Section II.C to address the traffic at issue, consistent with applicable service terms (Section II.B). In connection with traceback requests or related notifications, mitigation measures may also include implementing targeted mitigations associated with the traffic under review and coordinating mitigation steps with upstream providers where appropriate. In response to Commission-identified suspected illegal traffic, mitigation measures may also include taking applicable actions consistent with 47 C.F.R. § 64.1200(n)(2), which may include blocking (or ceasing acceptance of) the identified illegal traffic and substantially similar traffic on an ongoing basis where appropriate.

Upstream coordination. Where upstream-provider involvement is required for identification or mitigation of suspected traffic, Hotwire coordinates with its upstream provider consistent with Hotwire's escalation procedures and applicable service terms. Where that review identifies concerns warranting upstream actions, Hotwire escalates the matter to the upstream

provider for investigation and remediation and may suspend or terminate acceptance of traffic (or the relationship) where issues are not resolved.

II.F Regulatory History and Enforcement Matters

Hotwire, including its subsidiaries, affiliates, and any other related entities within the scope of the Robocall Mitigation Database (RMD) certification requirements, has not, at any time in the prior two years, been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or due to a deficient RMD certification or mitigation program description.

II.G Designated Robocall Mitigation and Traceback Contact

The name, title, department, business address, telephone number, and email address of the person within Hotwire responsible for addressing robocall mitigation-related issues, including traceback inquiries from the FCC, the ITG, and law enforcement agencies, is as follows:

Contact Name: Antonio Contarini
Contact Title: General Counsel
Contact Street: 2100 West Cypress Creek Road
Contact City: Fort Lauderdale
Contact State and Zip Code: FL 33309
Contact Telephone Number: (954) 406-1154
Contact Email: antonio.contarini@hotwiremail.com

Employee training and plan distribution. Hotwire has implemented a training program to ensure that employees receive appropriate training on issues related to illegal robocalls. Each member of the Hotwire NOC Department will receive a copy of this Robocall Mitigation Plan for their review and records. Hotwire's Human Resources department will also include this Robocall Mitigation Plan in its package of policy documents and other relevant materials distributed to relevant employees. Through this approach, Hotwire will seek to ensure that each of its employees is aware of the contents of this Robocall Mitigation Plan, thereby increasing its effectiveness. Hotwire's customer support personnel receive role-appropriate training on available robocall-related features.

II.H Plan Updates and Future Commitments

Hotwire will review and update this Robocall Mitigation Plan, and update its associated RMD filing information, within 10 business days to reflect any changes to required RMD content (including FCC Commission Registration System ("CORES")-sourced information), including changes to Hotwire's voice services, customer onboarding processes, monitoring and

**Hotwire Communications, Ltd.
Robocall Mitigation Plan**

mitigation controls, traceback participation processes, or upstream-provider arrangements. Additionally, Hotwire will recertify annually in the RMD by the March 1 deadline each year.

Exhibit A – Company Information

Company Name	FRN(s)	DBA and “Formerly Known As” Names
Hotwire Communications, Ltd.	0009846494 0031866437 0031866486	Hotwire Fision FisionX
Hotwire Communications, LLC	0025845058	Hotwire
Hotwire Infrastructure Group LLC	0032218133	Hotwire Communications Hotwire Fision FisionX
HWCA LP	0031328792	Hotwire Communications Hotwire Fision FisionX
HWAZ LLC	0034299644	Hotwire Communications Hotwire Fision FisionX
HWNV LLC	0034971093	Hotwire Communications Hotwire Fision FisionX
HWTX LLC	0032329021	Hotwire Communications Hotwire Fision FisionX

Hotwire and the entities listed in this Exhibit operate under Operating Company Number (“OCN”) 864K, which is the OCN reflected in Hotwire’s Robocall Mitigation Database filing for this Plan.

**Hotwire Communications, Ltd.
Robocall Mitigation Plan**