

UNITED STATES TELECOMMUNICATIONS CORPORATION

300 New Jersey Avenue NW, Suite 300, Washington, DC 20001-2030

(202) 380-2000 | www.ustelco.com

Robocall Mitigation Plan

Submitted in accordance with the requirements of the **Federal Communications Commission's Robocall Mitigation Database** pursuant to the TRACED Act and 47 CFR § 64.6305(c)

Prepared by: Office of the Chief Compliance Officer

Effective Date: March 21, 2025

Version: 1.0

Point of Contact: compliance@ustelco.com

1. Executive Summary

United States Telecommunications Corporation (USTelco) is committed to combating illegal robocalls and protecting the integrity of voice communications. This Robocall Mitigation Plan outlines the comprehensive, company-wide measures USTelco has implemented to prevent the origination and transmission of unlawful robocalls on its network. USTelco’s approach is proactive and multi-layered, combining industry-standard call authentication, strict customer vetting, real-time network monitoring, and advanced analytics (including AI-driven voice and traffic pattern analysis) to significantly reduce unwanted and illegal calls. In alignment with the TRACED Act and FCC regulations, USTelco has taken “*specific, actionable steps*” to stop illegal robocalls at the source, and this plan serves as our formal certification of those ongoing efforts.

USTelco provides a broad range of voice services, including enterprise SIP trunking, wholesale VoIP termination, DID origination, Bring-Your-Own-Carrier (BYOC) solutions, and AI-driven compliance systems, and this plan applies uniformly across all of them. We summarize below our corporate philosophy on robocall compliance, the technical architecture and protocols in place (such as STIR/SHAKEN call authentication), and the mitigation practices for both inbound and outbound traffic. We also detail our stringent customer and supplier onboarding standards, continuous monitoring and enforcement mechanisms, data retention and audit processes (including a blockchain-backed compliance ledger), collaboration with industry traceback and law enforcement efforts, integration of artificial intelligence technologies (e.g. voice fingerprinting), and our governance framework for continuous improvement. This document is intended as a formal, regulatory-facing submission demonstrating USTelco’s unwavering commitment to robocall mitigation and compliance with FCC, FTC, and other legal requirements.

2. Corporate Compliance Philosophy

USTelco’s corporate philosophy centers on a zero-tolerance stance toward illegal robocalling and a deep commitment to regulatory compliance. We recognize that unlawful robocalls are not only a nuisance but a serious threat to consumers, robocalls remain the top consumer complaint to the FCC and cost Americans billions

in scams. Protecting subscribers and the public from these harms is integral to our mission. USTelco’s leadership has established a culture of compliance that prioritizes ethical conduct, consumer privacy, and the integrity of our network. All levels of the organization, from executives to network engineers, share responsibility for enforcing robocall mitigation policies, and employees receive regular training on legal requirements (such as the TRACED Act, Telephone Consumer Protection Act (TCPA), and related FCC/FTC rules).

Our compliance philosophy is guided by the principle of “*doing the right thing*” proactively rather than merely reacting to enforcement. This means USTelco goes beyond basic legal obligations to implement best practices recommended by industry and government. We adhere fully to FCC regulations, including the mandate to maintain an effective robocall mitigation program, and we comply with the FTC’s Telemarketing Sales Rule and Do-Not-Call (DNC) Registry requirements to protect consumers from unwanted telemarketing. USTelco’s internal policies explicitly prohibit the use of our services for any illegal or nuisance calling. We require all customers, partners, and employees to uphold these standards. If there is any indication of non-compliance or abusive calling, USTelco acts swiftly to investigate and remediate the issue. In summary, our philosophy is one of **active compliance and consumer protection**, viewing regulatory frameworks not as obstacles but as vital tools to maintain trust in telecommunications.

3. Network Architecture and Call Authentication Protocols

USTelco has built a robust network architecture that integrates call authentication at its core to prevent caller ID spoofing and ensure tracebackability of calls. A key component of our architecture is the implementation of the STIR/SHAKEN framework, an industry-standard protocol for caller ID authentication across IP networks. USTelco is an authorized participant in the STIR/SHAKEN ecosystem, holding the necessary Service Provider Code (SPC) tokens and certificates to sign and verify calls. All SIP traffic originating on USTelco’s network or passing through our switching facilities is interfaced with STIR/SHAKEN authentication services. We attest each outbound call at the highest appropriate level based on how well we know the customer and the calling number: **Full Attestation (A)** for calls originating from numbers we assigned or whose user identity we can fully verify, **Partial**

Attestation (B) for calls from known customers using numbers we cannot fully verify (intermediate attestation scenarios), and **Gateway Attestation (C)** for calls that enter our network with no prior identification (though USTelco minimizes acceptance of such traffic). By signing outbound calls, we provide assurance to terminating carriers that the caller ID has been authenticated, thereby restoring trust in the caller ID display. Similarly, inbound calls to USTelco’s network are verified using STIR/SHAKEN, calls arriving without a valid signature or with a failing attestation are treated with heightened scrutiny or may be rejected outright if deemed suspicious.

Our network architecture consists of secure Session Border Controllers (SBCs) and media gateways that are configured to perform real-time call analytics and authentication. These systems are interconnected with our STIR/SHAKEN authentication service platform. USTelco operates as an **intermediate attestation authority** in cases where we are not the originating provider, ensuring that even transit traffic is signed with an appropriate attestation rather than passed unsigned. This involves validating the source of the call (through our know-your-customer procedures) and applying our digital signature before forwarding the call toward its destination. In addition to STIR/SHAKEN, USTelco’s architecture employs encryption and secure protocols where feasible (e.g., TLS for SIP signaling) to prevent tampering with call identity information. Our switches and routing infrastructure are designed to check each call against multiple databases and rulesets as the call setup occurs. This includes querying local and industry-wide “*Do Not Originate*” lists for numbers that should never originate traffic (such as government or invalid numbers) – any calls spoofing such numbers are blocked at our network edge. We have also integrated call identity analytics: if an originating party’s calling behavior triggers red flags (e.g., malformed caller ID data or inconsistent signaling), the call may be diverted for further verification or dropped.

USTelco’s call authentication deployment extends across all of our service offerings. For **enterprise SIP trunking** clients, we provide support for signing their outbound calls on their behalf and verifying inbound calls to their PBXs. For **wholesale VoIP termination**, all incoming traffic from customers (including other carriers or resellers) must pass through our authentication checks before we send it onward to terminating networks. In our **DID origination** services, every number we allocate

to customers is registered and tracked so that any call presented with that number can be confidently attested; similarly, we verify that customers have the right to use any telephone number they signal. In **BYOC solutions**, where enterprises supply their own carrier interconnect, we ensure that our network interconnects honor STIR/SHAKEN and other authentication handshakes, working with those third-party carriers as needed to maintain call identity information. Underpinning all of this is a resilient and scalable architecture: redundant servers for certificate management, real-time databases for storing attestation decisions, and continuous monitoring of the health of our STIR/SHAKEN signing and verification functions. This ensures that call authentication operates effectively without introducing significant latency or points of failure in call processing. In summary, USTelco's network is designed to **verify caller identity at every stage**, using the latest protocols and a secure architecture to make it difficult for illegal spoofed robocalls to traverse our system undetected.

4. Inbound and Outbound Robocall Mitigation Practices

USTelco employs rigorous robocall mitigation practices for both inbound calls (calls entering our network destined for our customers or downstream carriers) and outbound calls (calls originated by our customers or traversing our network towards other carriers). Our goal is to intercept and neutralize illegal or unwanted robocalls in either direction.

Outbound Mitigation: For calls originating from USTelco's customers or platforms, we have multiple safeguards in place to prevent illegal robocall traffic from ever leaving our network. First, every outbound call is screened through our authentication and analytics systems before routing. Calls are checked for valid caller ID presentation, if a customer attempts to send a call with a caller ID number that they are not authorized to use or that fails our number validation checks, the call is blocked or flagged for manual review. We maintain an internal registry of numbers (DIDs) that each customer is permitted to use, and we verify this on each call attempt. USTelco also utilizes **real-time spam call analytics** and pattern recognition on outgoing traffic: for example, our system monitors calling patterns such as extremely high volumes of short-duration calls, rapid sequential dialing through number blocks, or bursts of calls outside normal business usage. If a particular

outbound traffic stream exhibits known indicators of robocall campaigns (e.g., hundreds of calls per minute to diverse area codes, or calling patterns matching scam techniques), our system can automatically intercept those calls. We leverage both internal algorithms and external data (such as industry-provided lists of suspect numbers or fingerprinted scam audio content) to classify call attempts. Calls deemed likely illegal, such as those matching the signature of a known robocall scam, are dropped before completion or placed in a mitigation queue for investigation. Additionally, all outbound calls that fail STIR/SHAKEN attestation or validation (for instance, if our signing service cannot attest to the call’s legitimacy) are handled according to predefined policy: they may be transmitted with a lower attestation and a SHAKEN “verification failure” indicator to alert the terminating carrier, or they may be blocked if policy dictates (especially for international gateway scenarios where unauthenticated calls are high-risk).

Critically, USTelco enforces strict **Do-Not-Call (DNC) compliance** on outbound calling. We require that any marketing or informational campaigns carried out by our enterprise customers use scrubbed calling lists that honor the National DNC Registry and any internal opt-out lists. Our systems provide tools or APIs for customers to upload their DNC-suppressed lists, and we perform random audits of high-volume callers to ensure they are not contacting numbers on the DNC list without proper consent. Furthermore, USTelco implements opt-in verification for certain types of high-risk automated calls: for example, if a customer is sending pre-recorded messages (allowed only with consent under TCPA), we may require them to demonstrate that they have obtained and documented prior express consent from those consumers. Any customer found to be repeatedly violating DNC or consent requirements will have their campaigns halted and may face account termination under our enforcement policies (detailed in Section 6). By combining authentication, behavior analysis, and regulatory compliance checks, our outbound robocall mitigation practice ensures that illegitimate traffic is stopped at origination, before it can affect end users or lead to enforcement actions.

Inbound Mitigation: For calls coming into USTelco’s network (for instance, calls destined to our DID origination clients, enterprise PBXs, or being passed through our wholesale transit network), we apply an equally diligent screening process to shield end users from known robocallers and scams. Every inbound call handed to

us from another provider is subjected to STIR/SHAKEN verification when available. If the incoming SIP INVITE contains a STIR/SHAKEN Identity header, our verification service checks the digital signature and attestation level. Calls failing verification (e.g., the signature is invalid or the certificate is not trusted) are marked as suspect; we may choose to reject such calls or label them (e.g., inserting a warning in the caller ID display for our end-user subscribers or enterprise customers) depending on the context and customer preferences. Even for calls that pass STIR/SHAKEN, we perform additional analytics. USTelco subscribes to **dynamic robocall threat intel feeds** and maintains an internal blocklist of numbers and SIP signaling patterns linked to illegal robocall campaigns. If an inbound call's calling number appears on a known spam/robocaller list or exhibits a fingerprint of a robocall (for example, the audio of the call matches a known scam recording we have on file, or the call is one of many concurrent attempts from a single source), our system can automatically block it or divert it to a spam quarantine (such as voicemail or an interactive CAPTCHA system when applicable). We also utilize **caller reputation scoring** for inbound calls: through internal data and third-party analytics, each calling number is assessed for its likelihood of being fraudulent or spam. Low-reputation calls can be intercepted or annotated (e.g., flagged as "Spam Likely" for the recipient).

For inbound traffic that USTelco carries on behalf of other carriers (in our wholesale transit capacity), we adhere to industry best practices and FCC requirements to not carry obviously illegal traffic. This includes blocking calls from upstream providers that are not registered in the FCC's Robocall Mitigation Database or that we know to be sources of illegal calls. In practice, USTelco will refuse to accept inbound traffic from any carrier or VoIP provider that has failed to certify a robocall mitigation plan in the FCC database, as required by FCC rules. Additionally, we implement inbound **rate limiting and anomaly detection** – if an upstream source suddenly sends an unusual spike of calls through our network, our NOC (Network Operations Center) is alerted to investigate the nature of that traffic. Potentially harmful traffic (such as a sudden barrage of short-duration calls indicative of war-dialing or TDoS attacks) will be throttled or blocked. By maintaining these inbound controls, USTelco not only protects its direct customers but also contributes to the broader ecosystem's effort to shut down illegal call campaigns.

In summary, whether a call is entering or exiting USTelco’s network, it faces multiple layers of scrutiny. We **block or mitigate calls** that are identified as illegal, spoofed, or unwanted at various checkpoints: call signaling authentication, caller ID reputation analysis, known bad-number blocklists, real-time pattern analytics, and regulatory list compliance. These inbound and outbound practices work in tandem to ensure that USTelco is not a source or a conduit for unlawful robocalls, while still allowing legitimate traffic to flow uninterrupted.

5. Customer and Supplier Onboarding Standards

USTelco employs **best-in-class onboarding and vetting procedures** to prevent illegal robocallers from gaining access to our network. These procedures incorporate *Know Your Customer (KYC)*, *Know Your Business (KYB)*, and *Know Your Supplier (KYS)* frameworks, ensuring thorough due diligence for all clients and partners. By rigorously verifying identities and credentials at onboarding and through ongoing monitoring, USTelco aligns these practices with our robocall mitigation objectives and regulatory obligations (e.g. the TRACED Act and FCC rules. All vetting data is securely logged, retained, and continually analyzed to proactively identify and disqualify bad actors, reinforcing our commitment to compliance and our certification in the FCC Robocall Mitigation Database.

Know Your Customer (KYC) – Customer Identity Verification

Scope: USTelco performs KYC due diligence on **all new and existing customers**, including enterprise clients and wholesale carrier customers. This ensures we definitively know who is using our services and can hold them accountable. **Identification documentation** is collected and verified for the individual customer or the authorized representatives of business customers. This includes government-issued photo ID for persons (if applicable), full legal name, date of birth, and contact information of responsible officers or signatories. For business accounts, KYC also extends to identifying principal owners or executives to understand who controls the organization.

Verification: We validate each customer’s identity information through **authoritative sources and databases**. For individuals, this may involve using third-

party identity verification services or government resources to confirm the ID's authenticity and match to the person. For businesses, we cross-check the provided names of owners/agents against watchlists such as the U.S. Treasury's OFAC sanctions list and other law enforcement or anti-fraud databases to ensure no prohibited or high-risk persons are involved. We also confirm contact details (phone, email, physical address) by requiring reachable, legitimate points of contact. **Any discrepancies or red flags** (e.g. alias names, P.O. box as sole address, mismatched information) trigger enhanced due diligence, such as requesting additional proof or explanations.

Ongoing Monitoring: KYC is not a one-time event – USTelco continuously monitors customer identity status and behavior. We maintain updated records of authorized contacts and may require customers to re-verify information periodically (for example, if identification documents expire or if there are changes in ownership). In addition, we track external alerts (such as new sanctions or law enforcement actions) that could implicate a customer. If a customer's responsible parties become subject to legal restrictions or if we observe suspicious account behavior tied to an identity (e.g. multiple accounts using the same ID, or sudden changes inconsistent with the provided profile), we promptly review the account.

Disqualification Protocol: A customer **failing KYC checks** or later **found to have falsified information or engaged in illicit calling activities** is subject to immediate service suspension and disqualification. USTelco will deny activation to any applicant that cannot fully satisfy our identity verification requirements, and we terminate existing relationships if a customer's identity is no longer trustworthy or legal. These actions are documented and reported as necessary, in line with our commitment to keep bad actors off the network.

Know Your Business (KYB) – Customer Business Credentials and Purpose

Scope: In tandem with KYC, USTelco applies KYB vetting to **all business customers** (including enterprise clients and wholesale customers that are other voice providers or resellers). KYB focuses on verifying the legitimacy and details of the customer's business itself. This process ensures that each organization we serve is a

bona fide entity with a valid business purpose, consistent with lawful calling practices.

Documentation Requirements: Enterprise and wholesale customers must provide **official business documentation** during onboarding. Required documents include:

- *Proof of legal formation and good standing* – e.g. articles of incorporation or organization, state business registration certificates, or equivalent legal charter. We may also request a certificate of good standing from the jurisdiction of incorporation to confirm the business is active and in compliance.
- *Employer Identification Number (EIN)* or tax identification – the federal Tax ID is collected and verified against official records to confirm it matches the business name and entity type on file.
- *Business address and contact information* – the principal physical business address (no P.O. boxes) and main place of operations must be provided, along with a business telephone number and domain-based email addresses for contacts (to ensure they are tied to the company).
- *Ownership and management details* – a list of principal owners or executives and controlling interests. This helps ascertain who runs the business and allows cross-checking those individuals as part of KYC.
- *Nature of business and service usage* – a description of the customer’s industry, business model, and the intended use of USTelco’s voice services (e.g. outbound call campaigns, call center operations, resale of VoIP, etc.). This information is used to assess risk (for instance, high-volume telemarketing operations may warrant additional scrutiny and safeguards).

Verification: USTelco **validates each business customer’s credentials** through reliable sources. We confirm the company’s registration and good standing via government business registries (such as state Secretary of State databases or international business registries for foreign customers). The provided EIN is cross-checked against IRS records or third-party business identity services for consistency.

We also verify the business address (for example, using postal address databases or requesting utility bills to prove location if needed) and ensure the domain of contact emails corresponds to the company's website or known domain. As part of due diligence, USTelco reviews publicly available information about the business: we may examine the company's website, look for a visible customer base or product/service offerings, and search for any **negative signals** (such as prior regulatory violations, news of illegal robocalling incidents, or inclusion on industry watchlists). Additionally, we screen the business's name and principals against national and global sanction lists, fraud databases, and any FCC-provided lists of suspect entities. If the customer is itself a voice service provider or reseller, we confirm that they have complied with relevant FCC requirements (for example, having a Section 214 authorization if applicable, or having registered in the FCC's Robocall Mitigation Database if required). Only once all these checks are satisfactorily passed will the business customer be approved for service.

Ongoing Monitoring: USTelco continuously **monitors the status and activities of business customers** to ensure ongoing compliance. We require customers to promptly inform us of any material changes (e.g. ownership changes, name changes, mergers/acquisitions, or changes in the nature of their call traffic). We also perform periodic reverification of key KYB data – for instance, confirming annually that the customer's business remains in good standing and renewing any expired documents on file. Our team keeps abreast of industry tracebacks and enforcement actions; if a business customer is ever implicated in illegal robocalling or cited by regulators, we immediately re-assess their suitability. We analyze calling patterns and volumes relative to the customer's stated business use: unexpected surges in call traffic, abnormal call duration patterns, or traffic to high-risk destinations can indicate misuse that triggers an investigation. **Disqualification Protocol:** USTelco maintains a zero-tolerance approach for businesses that engage in illegal calling or misrepresent themselves. If a customer's business credentials **cannot be verified or are found fraudulent**, service is not activated (or is terminated if already active). Likewise, if a business customer is **found to be originating unlawful robocalls, violating our terms of service, or failing to meet ongoing KYB/KYC obligations**, we will deactivate their trunks and deny further access to our network. Such customers are reported to law enforcement or regulatory authorities as required.

These steps ensure that entities which pose a robocall risk are swiftly cut off, protecting both USTelco and the broader public.

Know Your Supplier (KYS) – Upstream Partner Due Diligence

Scope: USTelco extends rigorous vetting to all **upstream suppliers, interconnect partners, and voice service providers** with whom we exchange traffic. This *Know Your Supplier (KYS)* process (sometimes also referred to as KYB for partners) applies to any entity that sends calls into our network or carries our traffic upstream. It encompasses wholesale carriers we purchase services from, interconnecting voice providers (domestic or international), and any transit or gateway providers in our supply chain. The goal is to ensure that **every partner in our call path is trustworthy and compliant**, so that illegal robocall traffic is not introduced via third parties.

Upfront Vetting: Before onboarding an upstream partner or supplier, USTelco conducts a comprehensive review similar to our customer KYB process. We **collect and verify the business information of the supplier**, including: official legal name and corporate registration details, principal address of operations, jurisdiction of incorporation, corporate officers/contacts, and relevant identification numbers (such as an FCC Registration Number, 499-Filer ID for US carriers, or an international carrier license number where applicable). We require evidence of their regulatory status and good standing – for example, USTelco will only partner with domestic voice service providers that have complied with FCC mandates (such as STIR/SHAKEN implementation or, if applicable, a filed robocall mitigation plan in the FCC’s database). **FCC Robocall Mitigation Database Verification:** A critical step is confirming that any US-based or foreign provider in our supply chain is listed in the FCC’s Robocall Mitigation Database (as required by FCC rules for originating/facilitating providers). We obtain the supplier’s FCC Registration or verification from the database and ensure their certification is up-to-date, indicating they have implemented effective call authentication or mitigation measures. If a prospective partner is not in the database (when they should be) or has a history of non-compliance (e.g. was removed or is subject to an FCC blocking order), USTelco will not establish a connection. Additionally, we perform checks against **sanction lists and industry warnings** for suppliers: for instance, if the partner is a foreign

telecom, we ensure they are not from a sanctioned jurisdiction or flagged by U.S. authorities. We also review any available reputation indicators (such as known traffic profiles or if the Industry Traceback Group or FCC has previously identified them as a source of illegal calls).

Contractual Compliance: As part of KYS, USTelco enters into formal agreements with each interconnect partner that include **robocall mitigation commitments**. Our contracts require upstream suppliers to abide by all applicable laws and FCC rules on illegal robocalls, to perform KYC/KYB on their own customers, and to promptly cooperate in tracebacks and blocking of abusive traffic. We verify that partners have appropriate **internal controls** (e.g. they monitor their network for robocall activity and enforce their own mitigation policies). For higher-risk partners or routes, we may start with limited traffic or a trial period while closely observing call patterns.

Ongoing Monitoring: USTelco actively **monitors the quality and content of traffic** received from or sent through upstream partners. This includes analyzing call signaling and metadata for signs of illegal robocalling (such as spoofed numbers, high volume of short-duration calls, consecutive numbering, etc.). We track complaint metrics and traceback notices: if any calls handed off by an upstream partner are identified by industry traceback efforts as illegal, we immediately notify the partner and investigate. We maintain an ongoing dialogue with suppliers to address any issues; reputable partners are expected to quickly mitigate and block offending downstream customers on their end. USTelco also periodically refreshes the due diligence information for suppliers – for example, confirming their FCC filings remain current and checking if any new enforcement actions or public warnings have been issued against them. We subscribe to FCC orders and industry bulletins so that if a particular provider is ordered to be blocked (due to non-compliance or egregious robocall facilitation), we can take immediate action.

Disqualification Protocol: If an upstream supplier or interconnect partner **fails to meet our KYS standards or later violates them**, USTelco takes prompt corrective measures. This can include rejecting or quarantining traffic from that source until issues are resolved, or outright terminating the peering/contract for cause. In practice, USTelco will **cease accepting traffic from any provider that the FCC has identified for blocking** or that demonstrates an inability or unwillingness to control illegal traffic. Partners who refuse to cooperate in traceback investigations,

who are found sending us persistently illegal robocall campaigns, or who lose their authorized status (e.g. removed from the Robocall Mitigation Database or other accreditation) will be disconnected. All such actions are documented in our compliance records. By strictly policing our upstream routes, we ensure that our network does not become a gateway for unlawful calls originating elsewhere, thereby upholding the integrity of the call ecosystem.

Record-Keeping and Proactive Mitigation

All data collected through the KYC, KYB, and KYS processes is **securely logged and retained** in accordance with our record-keeping policies. USTelco maintains these records for the life of the customer or partnership and for a substantial period afterward (to meet any regulatory audit requirements and support investigations). This includes copies of identification documents, business certificates, verification results, contact logs, and notes on any risk flags or decisions. The stored data is handled confidentially and with appropriate access controls, but is readily available to support traceback requests or law enforcement inquiries if needed.

Importantly, USTelco uses its vetted data and ongoing monitoring results to drive **proactive mitigation**. We regularly analyze customer profiles and traffic patterns in tandem – for example, correlating a sudden surge in call complaints to the responsible account using our KYC/KYB info to immediately reach out or shut down service. Our compliance team conducts trend analysis across the customer base to spot any **repeat indicators of abuse** (such as multiple customers sharing a suspicious address or intermediary, or reuse of identifying information linked to past bad actors). These analytics help us preemptively identify emerging bad actors **before** they can cause significant harm. If any such patterns are detected, we escalate to manual review and, if warranted, swiftly **disqualify the entity from our network**. By leveraging comprehensive KYC/KYB/KYS data in this way, USTelco not only reacts to known illegal robocall incidents but actively works to **prevent them upfront**, fulfilling the due diligence expectations of the TRACED Act and reinforcing our status as a trustworthy voice service provider in the FCC’s Robocall Mitigation Database. Through these rigorous onboarding, vetting, and monitoring practices, USTelco ensures a highly secure and compliant network, barring bad actors and supporting industry-wide robocall mitigation efforts.

6. Monitoring, Detection, and Enforcement Mechanisms

USTelco has deployed a multi-faceted monitoring and detection system that continuously analyzes call traffic across our network to identify and mitigate illegal or suspicious calling activity in real time. These mechanisms enable us not only to detect anomalous or malicious call patterns, but also to enforce our policies through prompt action against offending calls or customers. Below we outline our approach to monitoring and the enforcement steps we take when issues are detected.

Real-Time Network Monitoring and Analytics: USTelco’s Network Operations Center (NOC) utilizes advanced call analytics tools to oversee voice traffic 24/7. Every call passing through our switches generates a call detail record (CDR) and associated signaling data that feed into our analytics engine. We employ **call pattern detection algorithms** that learn expected traffic profiles for each customer and trunk. If a customer that normally makes, say, 1,000 calls per day suddenly attempts 100,000 calls in an hour, or if calls are being made to an unusually broad set of area codes that were not previously in their profile, our system will flag this for immediate review. We also use **reputation-based scoring** for outgoing calls, where available: integration with industry databases lets us know if a calling number or a SIP identity has been associated with spam in the past. In addition to automated thresholds, the NOC team monitors alerts for specific known scam signatures (for example, spikes in short-duration calls that often indicate automated dialers detecting voicemails, or repeated calls with identical audio fingerprints as known scam robocalls).

USTelco leverages both in-house developed AI models and third-party analytics platforms to enhance detection. Our AI-driven anomaly detection (detailed further in Section 9) can pick up subtle patterns that rules might miss, for instance, detecting multiple customers suddenly calling the same set of numbers which could indicate a snowshoe spamming operation. We also keep an updated **blocklist and allowlist** database. Known bad actor numbers (such as those on FCC/FTC published scam number lists or our own internal list of numbers that have resulted in complaints) are automatically blocked if our network sees attempts to use them. Conversely, critical and emergency numbers (like 911 or official notifications) may be allowlisted to ensure they are never inadvertently blocked by an automated system. For inbound calls, as mentioned, we check STIR/SHAKEN verification status and mark calls

accordingly. Calls with attestation “C” (gateway attestation) or no attestation are monitored more strictly for other risk factors (e.g., if an unsigned inbound call is also from a number with a poor reputation score, it is very likely to be blocked or diverted).

Enforcement Mechanisms and Response: When our monitoring systems detect traffic that is likely illegal or violates our policies, USTelco takes immediate enforcement action to mitigate any potential harm. Enforcement can operate at the **call level**, **customer level**, or **network level** as appropriate:

- *Call-Level Blocking:* Suspicious calls are often automatically blocked or tagged by our system. For example, if a single call attempt is flagged as matching a known illegal robocall pattern or appears to spoof a number on a Do-Not-Originate list, our system will reject that call before it leaves/enters our network. The event is logged (with details such as timestamp, calling/called number, and reason for block) in our audit system for review. In cases of uncertainty, we may use call intercepts (e.g., playing a challenge message requiring caller input) to differentiate human callers from bots.
- *Rate Limiting:* If a certain traffic pattern triggers alerts (such as volume above a threshold), our network can dynamically rate-limit the traffic from that source. This means we will temporarily restrict the number of calls per second a customer can send until a further review is done. Rate limiting prevents explosive robocall campaigns from propagating while we investigate the cause of the surge.
- *Customer Account Suspension:* USTelco’s policy is to **suspend or terminate service for any customer confirmed to be transmitting illegal robocalls**. Upon detection of suspect activity from a particular customer account, our compliance team is immediately engaged. We will typically reach out to the customer’s designated contact to inform them of the issue and to request an explanation. In parallel, we may suspend the customer’s outbound calling capabilities (except perhaps emergency calls) to halt any ongoing illegal traffic. The customer is required to respond and, if possible, demonstrate that the calls in question were not illegal (for instance, provide proof of consent

for a calling campaign, or identify a compromised system if they were unknowingly used by a spammer). If the explanation is inadequate or if the behavior clearly violates the law or our terms, USTelco will move to terminate the customer's service. Our contracts support immediate termination in cases of egregious abuse such as this. We also maintain an internal **watch list** of customers: any customer that has had a robocall incident (even if resolved) is flagged for heightened monitoring going forward. Repeat offenders or those who fail to correct issues are permanently disqualified from our network. USTelco will not provide service to any customer or reseller that has a history of unresolved robocall enforcement actions – such entities are subject to *rejection and disqualification* from onboarding (as noted in Section 5) and, if discovered post-onboarding, prompt off-boarding.

- *Upstream Carrier Enforcement:* If we detect illegal robocall traffic entering our network from an upstream provider or peer, we take action at the interconnect level. This could involve blocking the specific traffic stream (e.g., blocking calls from a specific trunk or source number coming from that peer) and notifying the upstream provider of the issue. We expect our partners to respond quickly and mitigate on their side. If they fail to act and the illegal traffic continues, we will escalate by blocking more of their traffic or terminating the peering relationship, and we may report the incident to the Industry Traceback Group and FCC if appropriate. Our duty to the ecosystem means we cannot allow an upstream partner to funnel illegal calls through us unchecked.
- *Collaboration and Reporting:* As part of enforcement, USTelco cooperates with industry and government enforcement (see Section 8). For example, if a particular robocall campaign is identified, we will report the details to the Industry Traceback Group or law enforcement as needed, providing them the evidence collected. In cases where we have had to terminate a customer for illegal robocalling, we retain records of the event (outlined in Section 7) and will share relevant information with enforcement authorities under proper legal process to aid in investigations or prosecution.

In designing our enforcement approach, USTelco emphasizes both **speed** and **deterrence**. Speed is essential, illegal robocall campaigns can do significant damage in a short time, so our automated blocks and human oversight aim to stop incidents as soon as they are detected (often in-progress). Deterrence is achieved by making clear to all customers that violating our robocall policies will result in swift loss of service and potential legal exposure. We believe that the combination of real-time detection and strict consequences creates a strong preventive effect: customers know that our monitoring is capable of catching abuse and that we will not hesitate to act. This deters would-be bad actors from using our services and keeps our network hostile to illegal robocalling activity.

7. Data Retention, Logging, and Audit Infrastructure

Comprehensive data retention and logging are critical to USTelco’s robocall mitigation strategy. We maintain a robust audit infrastructure that records call events, mitigation actions, and relevant metadata, ensuring we have an evidentiary trail for compliance verification and enforcement purposes. Our data practices balance thorough record-keeping with privacy and security considerations, and we leverage innovative technology (including blockchain) to guarantee the integrity of our logs.

Call and Traffic Data Logging: USTelco captures detailed records for all calls traversing our network. This includes standard Call Detail Records (CDRs) for every call (timestamp, originating and terminating numbers, call duration, routing information, etc.), as well as additional fields pertinent to robocall mitigation. For example, we log the STIR/SHAKEN attestation level and verification status for each call (if a call was signed with attestation A/B/C or if an inbound call passed/failed verification). We also log any analytics tags applied to the call, such as a spam score or a flag indicating the call was blocked or labeled as spam. When our system blocks or flags a call due to a robocall mitigation rule, the system generates a log entry specifying the reason (e.g., “blocked – number on DNO list”, “blocked – failed authentication”, “restricted – high spam score”). These logs are time-stamped and indexed per customer and network element, which allows quick retrieval during investigations.

Blockchain-Backed Compliance Ledger: To enhance the trust and tamper-resistance of our audit trail, USTelco utilizes a blockchain-backed repository for critical compliance data. Key events, such as instances of call blocking, attestation/signing records, and customer enforcement actions, are cryptographically hashed and written to a private, permissioned blockchain ledger. This ledger functions as an immutable timeline of our robocall mitigation activities. For example, if we block a batch of calls from a certain customer on a given date for suspected robocalling, a hash of the event details (customer ID, reason, number of calls, timestamp) is recorded on the ledger. This provides an extra layer of evidentiary support: if ever challenged or audited by regulators, USTelco can prove that certain actions were taken at certain times and that the records have not been altered. The blockchain ledger is maintained across multiple secure nodes and is access-controlled to authorized compliance personnel. While the detailed logs remain in our databases, the blockchain entries serve as an integrity check, ensuring our internal records can be verified for authenticity.

Data Retention Policy: USTelco’s policy is to retain robocall mitigation-related data for a sufficient period to support investigations and compliance checks by authorities. Unless otherwise directed by regulation, we retain call detail records and associated robocall mitigation logs for a minimum of **24 months**. This retention period is chosen to cover the typical statute of limitations for enforcement actions and to support historical analysis of calling patterns (some regulations or legal actions may have a window of a couple of years). In the event that a particular set of records is relevant to an ongoing investigation or subpoena, we will preserve those records as needed beyond the standard retention period (litigation hold). The blockchain ledger entries, being small in size (hashes), are kept indefinitely to maintain the continuity of our compliance chronology. Additionally, we store copies of our robocall mitigation plan versions, customer consent records (if provided by customers for their calling campaigns), and other compliance documents in secure archival storage.

Audit and Review Processes: Our infrastructure is designed not just to collect data, but also to facilitate regular audits. We have automated auditing scripts that periodically analyze log data to identify any irregularities or missed detections. For instance, if there were any instances where an illegal call might have not been

blocked, we want to catch and review those. We also audit our own actions, such as verifying that every call that should have been signed with STIR/SHAKEN was indeed signed, and that our systems are performing as expected. The blockchain ledger is cross-checked with internal logs to ensure consistency. USTelco's compliance team performs quarterly audits of random samples of call records and mitigation actions to ensure policy adherence. Any discrepancies or anomalies found in audits are documented and investigated, with remedial steps taken as necessary (e.g., if an audit finds a certain mitigation rule was not properly enforced for a subset of traffic, we fix the rule and consider it under our improvement process in Section 10).

Security and Privacy of Logs: We recognize that call logs can contain sensitive information (like phone numbers and call times, which might be considered Customer Proprietary Network Information - CPNI). USTelco protects its logging and audit systems with strict security controls. Access to detailed call logs is limited to authorized engineers or compliance officials on a need-to-know basis, and all access is logged. Data at rest in our log repositories is encrypted, and data in transit (for example, when transferring logs to the blockchain ledger or to an analysis system) is also encrypted. We comply with all relevant privacy laws and FCC CPNI rules in handling these records. Moreover, any sharing of log data with external parties (such as law enforcement or the Industry Traceback Group) is done in accordance with legal requirements and after ensuring proper confidentiality measures are in place.

In summary, USTelco's data retention and audit infrastructure provides a **comprehensive and reliable record** of our fight against illegal robocalls. By combining extensive logging with cutting-edge integrity measures like blockchain, we ensure that we can demonstrate our mitigation efforts to regulators and investigators with transparency and credibility. Our commitment to thorough record-keeping not only supports enforcement and accountability but also helps us continually refine our techniques by learning from past data.

8. Collaboration with Traceback and Law Enforcement Entities

Collaboration with industry traceback efforts and law enforcement agencies is a cornerstone of USTelco’s robocall mitigation program. We understand that the battle against illegal robocalls requires a coordinated approach across the telecommunications ecosystem, and USTelco is fully committed to doing its part. Our policies and procedures are designed to ensure rapid, transparent cooperation with the FCC-designated traceback consortium, as well as with federal and state authorities, in order to identify the sources of illegal calls and remove bad actors from all networks.

Industry Traceback Group (ITG) Participation: USTelco is an active participant in the Industry Traceback Group, the official consortium led by USTelecom that conducts tracebacks of suspected unlawful robocalls. We have formally registered with the ITG and adhere to its established policies and procedures for traceback cooperation. USTelco has designated a dedicated Traceback Response Team within our compliance department, including a primary point of contact who is available to promptly address traceback requests (contact information for this liaison has been provided in our FCC Robocall Mitigation Database filing as required). When we receive a traceback request from the ITG (or directly from an enforcement agency), we treat it with top priority. Our team will immediately query our logs and databases (as described in Section 7) to determine if the call(s) in question passed through our network and, if so, to identify the source (which customer or which upstream provider) and the call details. We typically can retrieve and relay information such as: the customer account that originated the call, the ingress/egress IPs or trunks, call timestamps, and any STIR/SHAKEN attestation info. USTelco responds to traceback inquiries within the requested timeframe (often within 24 hours or faster), providing the relevant information to the ITG in a secure manner. We understand that under U.S. law (specifically the TRACED Act), all voice providers are *“required by law to cooperate with traceback requests”* from the registered consortium, and we take that obligation seriously.

In addition to reactive cooperation, USTelco proactively supports the ITG’s mission. We participate in ITG-led initiatives and working groups to improve traceback processes and share best practices. Our company attends industry forums and training sessions on traceback to stay current on evolving techniques (for example, handling traceback for VoIP calls that might involve multiple IP hops or

international segments). Furthermore, if USTelco itself observes a pattern of illegal robocalls that we think would benefit from broader traceback (for instance, if multiple upstream sources are sending us similar scam traffic), we will reach out to the ITG to initiate tracebacks upstream of us. By being proactively engaged, we help accelerate the identification of the originators of illegal campaigns.

Cooperation with Law Enforcement and Regulatory Agencies: USTelco maintains open lines of communication with law enforcement agencies such as the FCC’s Enforcement Bureau, the Federal Trade Commission (FTC), and state attorneys general who are active in combating telemarketing fraud. When an enforcement authority serves us with a subpoena or request for information regarding suspected robocalls, we have procedures to respond efficiently and lawfully. Our compliance team, together with legal counsel, will authenticate the request and then draw upon our retained data (Section 7) to provide the requested evidence. This can include call records, customer contact information, and any other relevant logs. We ensure such disclosures comply with privacy laws and are narrowly tailored to the request. USTelco also voluntarily reports severe incidents to authorities. For instance, if we detect a large-scale scam (like a impostor government agency scam) targeting vulnerable individuals, we may notify the FCC or FTC of the incident and our actions taken, even if we have already stopped it on our network. We see ourselves as a partner to enforcement, not just a passive participant.

Additionally, USTelco complies with specific FCC directives related to robocall mitigation enforcement. This includes the new FCC requirements for providers to respond to “K4 Notices” (initial warning of suspected illegal traffic) and “K4 Notices”/“N2 Orders” (cease-and-desist orders) within mandated timeframes. Our plan ensures we would immediately investigate and respond to any such notice, providing confirmation of mitigation or the steps taken to block the traffic in question, as required by the FCC’s rules. We also coordinate with the FTC regarding the Do-Not-Call registry if needed – for example, if a major DNC violation is traced to a customer on our network, we will share information and take action accordingly.

Inter-provider and Industry Collaboration: Beyond formal tracebacks and law enforcement, USTelco collaborates with other carriers and industry groups to share information on robocall trends and mitigation strategies. We are a member of

telecom industry associations that focus on network security and fraud prevention. Through these channels, we exchange anonymized data or cautionary alerts about emerging robocall schemes (for instance, if a new robocall scam script is circulating, or if a particular calling number has been hitting many networks). This peer collaboration helps the entire industry stay ahead of criminals who often target multiple carriers. USTelco also supports the development of new standards and frameworks (such as updated STIR/SHAKEN enhancements for caller ID on non-IP networks, or richer call metadata for traceback) by contributing technical feedback and participating in pilot programs when applicable.

In summary, USTelco's approach is to be **transparent and cooperative** with all legitimate efforts to trace and prosecute illegal robocalling. We view compliance with traceback and law enforcement as more than just a legal duty, it's part of our corporate responsibility to the public. By actively collaborating with the ITG and authorities, we help ensure that when illegal calls do occur, they can be quickly traced to their source and dealt with, and we remove any such offenders from our own network without delay. This cooperation amplifies the effectiveness of our own mitigation measures by linking them into the broader enforcement ecosystem.

9. AI and Advanced Technology Integration

USTelco stays at the forefront of technological innovation in its fight against illegal robocalls. We have integrated advanced technologies, including artificial intelligence (AI) and machine learning, into our robocall mitigation systems to enhance detection accuracy and responsiveness. From real-time analytics to novel solutions like AI-driven voice *fingerprinting*, our use of technology multiplies the effectiveness of traditional mitigation techniques and allows us to adapt rapidly as scammers evolve their tactics.

AI-Powered Call Analytics: Traditional rule-based systems can struggle to catch every illegitimate call, especially as robocallers constantly adjust their methods. To address this, USTelco employs AI and machine learning models that analyze calling patterns and content in real time. Our AI models are trained on large datasets of calling behavior, including examples of both legitimate traffic patterns and known abusive patterns. The models identify subtle anomalies or correlations that might

indicate robocall activity – for example, an AI model might notice that several different customer accounts are calling the same unusual set of destination numbers within a short period (something a single rule might not catch). It might also detect changes in behavior, like a normally low-volume trunk suddenly initiating short, repetitive calls (possible sign of a bot dialer). The AI system assigns a **risk score** to call attempts or calling sessions based on dozens of variables. If the risk score exceeds a threshold, it triggers our mitigation actions (block or review), as described in Section 6. Importantly, our AI is adaptive: it uses feedback from enforcement outcomes to get smarter. If certain types of illegal calls got through undetected, we feed those instances back into training so the system learns from mistakes. Conversely, we strive to minimize “false positives” by refining models to recognize legitimate high-volume scenarios (for instance, automated appointment reminder calls which are legal and desired). The combination of AI-driven analysis with human oversight ensures a high catch-rate of bad calls while keeping normal traffic flows stable.

AI Voice Fingerprinting and Audio Analysis: One cutting-edge tool USTelco has invested in is **AI-based voice and audio fingerprinting**. Many robocalls use identical or very similar prerecorded messages – for instance, the infamous “vehicle warranty” scam calls often share the same female voice recording. Our system uses voice analysis algorithms to create a digital “fingerprint” of audio streams on calls. When a call is connected through our network, if it is terminated by the callee or passes through a media gateway, our system can sample a snippet of the audio (where legally permissible and solely for network security purposes). The AI then compares this audio fingerprint to a database of known illegal robocall audio patterns. This database is built from various sources: audio from honeypot lines, recordings provided by enforcement partners, and our own previously identified robocalls. If a match or a high-confidence similarity is found, it indicates the call is likely a repeat of a known scam robocall. Our network can then automatically flag or terminate such calls. For example, if an outbound call from a customer starts playing a message that matches the “IRS tax scam” recording fingerprint, our system will catch this in progress and stop the call, possibly before the message fully plays out to a victim. AI voice fingerprinting helps us go beyond metadata and actually scrutinize call content in a targeted, privacy-conscious manner (we do not listen to

or analyze any call content except for the purposes of detecting known illicit robocall messages, and we comply with legal requirements in doing so).

Machine Learning for Caller Reputation: We also use machine learning to maintain and update a dynamic **caller reputation scoring system**. This system aggregates information such as: how often do calls from a certain number result in immediate hang-ups? How many downstream carriers have flagged that number? Have we seen complaints or tracebacks involving that number or numbers with similar patterns? By using clustering algorithms, the system can even identify groups of numbers that behave similarly (for example, a rotating set of caller IDs used by one scam operation). These insights allow us to preemptively block or challenge calls from numbers that the AI model has determined are likely sources of robocalls. This is essentially an adaptive, AI-driven blacklist that updates continuously, far more quickly than a manual list could.

Integration of Third-Party Data and Tools: In addition to our in-house technologies, USTelco integrates respected third-party solutions to augment our capabilities. We partner with leading vendors in robocall analytics to incorporate their spam detection feeds, numbering databases, and algorithms into our platform. For instance, we use external datasets that provide real-time lists of high-risk numbers or predictive scoring for calls, blending that with our own AI's assessment. Our systems are built with open APIs that allow plugging in new analytic modules with ease. If a new technology emerges (for example, an AI tool that can detect AI-generated synthetic voices that scammers might use to impersonate people), we can pilot and integrate that tool. USTelco also watches developments in **blockchain** and identity verification technology beyond just our logging ledger – we are exploring blockchain-based caller ID verification systems that could, in the future, help validate the origin of calls in a decentralized manner.

Continuous Tuning and Human Oversight: We acknowledge that AI and advanced tools are powerful but not infallible. Therefore, USTelco maintains human oversight of these systems. Our network security analysts review the outcomes of AI detections regularly, verifying that the decisions made (blocks or allows) were appropriate. If the AI flagged something that turned out to be a false alarm, we adjust thresholds or retrain models to improve accuracy. Conversely, if an illegal call was missed, we analyze why and enhance the model. The AI systems produce

explanations or indicators (when possible) so our team can understand the basis of a decision. This transparency is important for trust and for fine-tuning the system.

By harnessing advanced technology, USTelco significantly strengthens its robocall mitigation posture. AI allows us to **stay ahead of evolving threats** – as robocallers change tactics, our systems learn and adapt in near-real time. Voice fingerprinting gives us a novel weapon to catch repeat offender calls that might slip through conventional filters. All these technologies are integrated into a cohesive platform that works in concert with our traditional mitigation measures. The result is a smarter, faster response to robocall threats, minimizing the window of opportunity for scammers to exploit telecommunications networks.

10. Continuous Improvement and Governance

Robocall mitigation at USTelco is not a “set-and-forget” program, but rather an ongoing effort subject to continuous improvement and strong governance oversight. We recognize that the regulatory landscape, technological tools, and robocalling tactics are constantly evolving. Therefore, USTelco has instituted a governance framework to regularly review and refine our robocall mitigation strategies, ensuring they remain effective and up-to-date. This final section outlines how we manage the ongoing evolution of our program and maintain accountability at the highest levels of the company.

Governance Structure: USTelco has a dedicated **Robocall Mitigation Governance Committee** that oversees the implementation and efficacy of this plan. The committee is composed of senior representatives from key departments: Network Operations, Compliance/Legal, Customer Operations, and Security. It is chaired by our Chief Compliance Officer (CCO) who reports directly to the CEO and Board of Directors on compliance matters. The committee meets on a regular basis (at least quarterly, with more frequent ad-hoc meetings if needed) to review robocall mitigation performance metrics and make policy decisions. Topics reviewed include: statistics on calls blocked or flagged, any incidents of illegal traffic that were identified, outcomes of any enforcement actions against customers, traceback requests handled, and any new risks or trends observed. The committee uses these reviews to assess whether our current measures are sufficient or if

adjustments are needed. For instance, if a new type of robocall scam is emerging industry-wide, the committee will task the technical teams to incorporate detection for that scam, or if regulations change, the committee ensures our practices are updated accordingly. This governance body also approves resource allocations (e.g., investment in new technology or personnel training) to strengthen the mitigation program.

Policy Updates and Adaptation: We maintain this Robocall Mitigation Plan as a living document. Any changes in FCC rules, such as new requirements for the Robocall Mitigation Database filing, or changes stemming from the TRACED Act or other legislation, are promptly reflected in our policies. For example, if the FCC were to tighten the definition of “reasonable steps” providers must take or introduce new required mitigation standards, USTelco would incorporate those into our plan and operations without delay. Our Compliance department keeps abreast of all relevant regulatory proceedings and industry best practice publications. USTelco is also mindful of developments in related areas like consumer protection laws and international robocall mitigation efforts (since scams can be globally sourced). On at least an annual basis, we perform a top-to-bottom review of the Robocall Mitigation Plan to evaluate its completeness and effectiveness, updating it as needed. Material updates are approved by the Governance Committee and, when required, re-submitted to the FCC’s Robocall Mitigation Database (for instance, in line with FCC mandates to periodically recertify and update filings).

Training and Internal Awareness: Continuous improvement also involves the human element – ensuring that our staff are well-informed and vigilant. USTelco conducts regular training sessions for employees in relevant roles (customer onboarding, network monitoring, support, etc.) on the latest robocall schemes and our mitigation procedures. New hires in technical and customer-facing departments are onboarded with our corporate compliance philosophy and taught how to spot and escalate potential robocall issues. We update training materials frequently to reflect new scam scenarios or tool enhancements (for example, if we deploy a new AI monitoring feature, the NOC team is trained on how it works and what its alerts mean). By keeping our teams educated, we create a workforce that serves as an additional layer of defense.

Customer and Industry Feedback Loop: USTelco values feedback from legitimate customers and industry peers to improve our practices. We provide channels for customers to report if they believe their outgoing calls are being incorrectly blocked or labeled, so we can investigate and fine-tune our filters (ensuring we minimize impact on lawful communications). We also monitor customer satisfaction and complaint metrics related to voice call delivery – a sudden uptick in complaints about blocked calls could indicate an overzealous filter that needs adjustment. On the flip side, we pay attention to any reports from consumers or authorities that a call through our network made it to a victim illegally; such an event triggers an internal post-mortem analysis on how it evaded our controls and what can be improved. Our participation in industry groups means we also learn from the experiences of others – if a new mitigation technique proves successful for others, we consider adopting it; if a certain approach caused issues, we take note to avoid pitfalls.

Audit and Accountability: As mentioned in Section 7, we conduct internal audits of our mitigation actions and logs. The results of these audits are reported to the Governance Committee. If an audit finds any gap or non-compliance with our stated procedures, it is flagged as an issue that the committee will address with a corrective action plan. USTelco’s executive leadership requires that robocall mitigation effectiveness be part of our key performance indicators for network integrity. In fact, metrics like “illegal calls blocked per quarter” and “time to respond to traceback” are tracked. These metrics not only show our success rate but also help identify trends (e.g., if the number of blocked calls is rising, are we seeing more attempts that need further action beyond blocking?). Our Board of Directors is briefed at least annually on robocall mitigation status as part of compliance and risk oversight, reflecting how seriously the company takes this issue at the highest level.

Continuous Technology Improvement: We continually invest in improving the technological tools described in this plan. This means regularly updating software (e.g., upgrading STIR/SHAKEN software to the latest versions and certificate practices), applying patches to security systems, and evaluating new vendors or solutions in the market. We allocate R&D efforts to test emerging ideas like voice analytics, or perhaps integrating with forthcoming industry initiatives (such as SHAKEN for international calls, when available). USTelco may run pilot programs

in a controlled environment for new mitigation technologies and, if successful, roll them into production. We also engage with standards bodies and consortiums – for example, contributing to discussions at ATIS/SIP Forum on how to extend caller ID authentication, or exploring cross-carrier data sharing frameworks to better identify robocall sources. By staying on the cutting edge, we ensure our mitigation toolkit does not become obsolete in the face of new robocall tactics.

In conclusion, USTelco’s robocall mitigation program is underpinned by a strong governance model and a philosophy of **continuous improvement**. We do not consider compliance a static checklist, but rather a dynamic process of learning and adapting. Through regular oversight, updating of policies, training, feedback incorporation, and technical upgrades, we strive to keep our defenses robust and one step ahead of bad actors. This continuous improvement and governance focus ensures that USTelco will remain an industry leader in robocall mitigation, providing reliable and secure voice services to our customers while actively supporting the broader effort to eliminate illegal robocalls.