

Tru Voip Robocall Mitigation Plan

Submitted in accordance with the TRACED Act and 47 CFR § 64.6305(c) for filing in the FCC Robocall Mitigation Database

Effective Date: July 22, 2025 **Version:** 1.0

1. Executive Summary

Tru Voip LLC is fully committed to combating illegal robocalls and protecting the integrity of voice communications on its network. This Robocall Mitigation Plan outlines the comprehensive, company-wide measures Tru Voip has implemented to prevent the origination and transmission of unlawful robocalls. Tru Voip'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 traffic pattern analysis) to significantly reduce unwanted and illegal calls. In alignment with the TRACED Act and FCC regulations, Tru Voip has taken **specific, actionable steps** to stop illegal robocalls at their source, and this document serves as our formal certification of those ongoing efforts.

Tru Voip provides a broad range of voice services as both a **voice service provider** and an **intermediate provider**, including enterprise SIP trunking, wholesale VoIP termination, DID origination, hosted PBX services, Communications Platform as a Service (CPaaS), and hosted cloud-based predictive dialers. This plan applies uniformly across all of these service offerings. We summarize below our corporate compliance philosophy, the technical architecture and protocols in place (such as STIR/SHAKEN caller ID authentication), and the mitigation practices employed for both outbound and inbound call traffic. We also detail our stringent customer onboarding and Know-Your-Customer (KYC) procedures, continuous monitoring and enforcement mechanisms, data retention and audit processes, collaboration with industry traceback and law enforcement efforts, integration of artificial intelligence technologies, and our commitment to continuous improvement. This plan is presented as a formal, regulatory-facing submission demonstrating Tru Voip's unwavering commitment to robocall prevention, regulatory compliance, and network integrity in accordance with FCC, FTC, and other legal requirements.

2. Corporate Compliance Framework

Tru Voip's corporate compliance framework is built on a zero-tolerance policy toward illegal robocalling and a deep commitment to all applicable regulations. Protecting consumers and the public from unlawful robocalls is integral to our mission. Tru Voip's leadership has

established a culture of compliance that prioritizes ethical conduct, consumer privacy, and the security of our network. All levels of the organization – from executives to network engineers – share responsibility for enforcing robocall mitigation policies. Employees receive regular training on legal requirements and industry best practices, including the TRACED Act, the Telephone Consumer Protection Act (TCPA), Telemarketing Sales Rule, and related FCC/FTC rules. This ongoing training and awareness ensure that our team stays current on evolving regulations and methods to combat illegal calls.

Our compliance philosophy is guided by the principle of being proactive rather than merely reactive. Tru Voip goes beyond basic legal obligations to implement best practices recommended by regulators and industry groups. We adhere fully to FCC rules – including the mandate to maintain an effective robocall mitigation program – and we comply with the FTC’s telemarketing regulations and Do-Not-Call (DNC) Registry requirements to protect consumers from unwanted calls. Tru Voip’s internal policies (embodied in our Master Service Agreement and Acceptable Use Policy) explicitly prohibit the use of our services for any illegal, abusive, or nuisance calling. We require all customers, partners, and employees to uphold these standards of lawful and responsible use. If there is any indication of non-compliance or abusive calling on our network, Tru Voip acts swiftly to investigate and remediate the issue. In summary, our corporate compliance framework fosters active compliance and consumer protection, viewing regulatory requirements not as obstacles but as vital tools to maintain trust in telecommunications. We enforce a “zero-tolerance” stance: any willful violation of robocall laws or our policies by a customer or employee is met with prompt enforcement action (up to and including service termination or disciplinary measures). Through strong top-down leadership and company-wide accountability, Tru Voip maintains a robust compliance culture dedicated to stopping illegal robocalls before they can harm end users or the public.

3. Scope of Services

Company Role: Tru Voip operates as both a *voice service provider* (directly providing voice communications services to enterprise and retail customers) and as an *intermediate provider* (carrying or routing voice traffic from other service providers). Our network and mitigation practices span both roles, ensuring that whether Tru Voip is originating, carrying, or terminating call traffic, robust robocall controls are in place.

Service Offerings: Tru Voip’s telecommunications services cover a wide scope to meet diverse customer needs. Key services include:

- **Enterprise SIP Trunking:** IP-based trunk services that connect business phone systems (PBXs) to the PSTN, supporting both inbound and outbound calling for enterprises.

- **Wholesale VoIP Termination:** High-volume voice termination services for other carriers, call centers, and service providers, where Tru Voip carries outbound calls to destinations worldwide.
- **DID Origination:** Provision of Direct Inward Dial (DID) numbers and inbound call delivery to customers (including toll-free and local numbers in various regions) to enable customers to receive calls through Tru Voip's network.
- **Hosted PBX and Unified Communications:** Cloud-based business telephony platforms (hosted PBX) and unified communications solutions where Tru Voip provides the switching infrastructure and feature set for customers' voice calls and messaging.
- **CPaaS (Communications Platform as a Service):** API-driven communication services that allow developers and customers to integrate voice calling (and messaging) into their own applications and workflows. Tru Voip's CPaaS offerings enable programmatic call initiation, interactive voice response, and other advanced telephony functions, all subject to our mitigation and monitoring controls.

Across all these services, Tru Voip's **network infrastructure is fully IP-based** and interconnected with upstream carriers and the public telephone network. The same robocall mitigation standards described in this plan are applied uniformly, regardless of service type. This means, for example, that whether a call originates from our SIP trunking customer, a hosted dialer, or is transiting our wholesale network, it is subject to the same caller ID authentication, vetting, and traffic monitoring measures. As an intermediate provider, Tru Voip also ensures that any traffic we carry on behalf of other providers meets our compliance standards – we do not allow our network to be used as a conduit for illegal robocalls. The **scope of this plan** therefore encompasses all Tru Voip voice traffic, inbound and outbound, across all product lines and customer types.

4. STIR/SHAKEN Implementation Status

Tru Voip is in the process of fully implementing the **STIR/SHAKEN** caller ID authentication framework across our network. We recognize STIR/SHAKEN as a critical industry-standard protocol (Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using Tokens) mandated by the FCC for IP-based voice service providers to

combat caller ID spoofing and illegal robocalls. Tru Voip has already taken substantial steps to participate directly in the STIR/SHAKEN ecosystem. We have obtained the necessary credentials – including Service Provider Code (SPC) tokens and digital

certificates – from the industry’s STI-Policy Administrator, enabling us to digitally sign and verify calls.

All SIP call traffic originating on Tru Voip’s network or passing through our switching facilities is being integrated with STIR/SHAKEN authentication services. We are configuring our Session Border Controllers and call platforms to sign each outbound call with the appropriate attestation level and insert a secure Identity header. Tru Voip will **attest** each outbound call at the highest level appropriate based on our relationship with the calling party and the number: for calls using numbers we assign or can fully validate, we will provide Full Attestation (“A”); for calls from customers using numbers not obtained from us (but for which we have verified user identity/authorization), we provide Partial Attestation (“B”); and we avoid handling traffic that would only merit Gateway Attestation (“C”) except when absolutely necessary. By signing outbound calls, Tru Voip adds a layer of trust to the caller ID – the called party’s carrier can verify that the call is authentic and not illegally spoofed.

On inbound calls, Tru Voip’s systems will check for STIR/SHAKEN Identity headers on SIP traffic and perform verification of each signed call’s digital signature. Calls arriving without a valid signature, or with an invalid/failing attestation, are treated with heightened scrutiny or may be rejected outright if deemed suspicious. This ensures that we do not terminate calls that have been flagged as potentially spoofed. Tru Voip is committed to **full STIR/SHAKEN deployment** and is actively working toward 100% coverage. We are upgrading network equipment and coordinating with our upstream and downstream partners to exchange signed call traffic wherever possible. During this implementation phase, Tru Voip continues to operate a robust robocall mitigation program (as described in this plan) for any calls that cannot yet be signed or verified. In short, Tru Voip will directly participate in STIR/SHAKEN as an authenticated service provider, holding our own certificates to sign calls and validate caller identities. This status and our ongoing STIR/SHAKEN efforts will be reflected in our FCC Robocall Mitigation Database certification.

5. Caller ID Authentication and Number Validation

Ensuring the authenticity and accuracy of Caller ID information is a core element of Tru Voip’s robocall mitigation strategy. We have established strict protocols to prevent caller ID spoofing and to validate the calling numbers used on our network:

- **Caller ID Screening:** Every outbound call through Tru Voip is automatically screened for a 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, our system will block the call or flag it for manual review. We maintain an internal registry of telephone numbers (DIDs) that each customer is permitted to use, and our outbound call processing verifies each call's caller ID against this registry in real time. This prevents malicious actors from spoofing numbers that they do not legitimately control.

- **Authorized Number Registry:** Tru Voip's internal number registry is built from multiple sources: numbers that we have assigned or ported in for the customer, numbers verified as belonging to the customer (with proof of ownership or assignment), and any legitimate toll-free or short code numbers registered to the customer. Customers are required to register all outgoing caller ID numbers with us. Any call attempt with a number not on the customer's approved list is automatically blocked. We also periodically audit active caller IDs against authoritative databases to ensure they remain valid and not revoked.
- **Truth-in-Caller-ID Compliance:** Tru Voip fully complies with the FCC's Truth in Caller ID regulations, which prohibit any spoofing of caller identity with intent to defraud, cause harm, or wrongfully obtain anything of value. Our Acceptable Use Policy explicitly forbids customers from falsifying or misrepresenting caller ID information; in particular, using a number as Caller ID that the customer does not own or have rights to is strictly prohibited. All call signaling and CNAM (Caller Name) data provided must be accurate and truthful. We employ technology to detect common spoofing techniques (such as neighbor spoofing, where a caller ID is chosen to match the first 6 digits of the called number) and will block or scrutinize such calls unless there is a valid reason for the matching exchange.
- **STIR/SHAKEN Call Authentication:** As noted in Section 4, Tru Voip is implementing STIR/SHAKEN across our IP network. In practice, this means every outbound call from our network that carries a North American Numbering Plan number in the caller ID field will be signed with our digital certificate (or that of an authorized signing partner until our own deployment is complete). The STIR/SHAKEN attestation affirms the caller ID has been authenticated by Tru Voip. Conversely, for inbound calls, we verify the STIR/SHAKEN signature when present and use that information as part of our decision-making for call handling. Calls that fail verification (indicating a likely spoofed caller ID) can be dropped or labeled as spam. This framework greatly enhances caller ID trust when interconnecting with other carriers.
- **Number Validation Protocols:** Tru Voip employs additional number validation protocols internally. We cross-check outbound caller IDs against known legitimate number ranges and databases. For example, if a call purports to originate from an area code/exchange combination that is not assigned to any carrier (or is unallocated), we will block it. We also enforce format and consistency checks (valid NANP numbers, no

obviously malformed numbers, etc.). Our systems integrate with external numbering data sources to validate that a given number is active and assigned. In the case of large customers or partners using their own number blocks, we may require letter-of-authorization documentation or other proof before allowing traffic with those numbers. These safeguards collectively ensure that **only valid, authorized caller IDs** are used on Tru Voip's network, greatly reducing opportunities for spoofing. Any attempt to present a false caller identity is caught by our checks and stopped before the call proceeds.

6. Know-Your-Customer (KYC) and Vetting Protocols

Tru Voip maintains stringent customer onboarding and vetting procedures to prevent bad actors from ever gaining access to our services. Our **Know-Your-Customer (KYC)** program, alongside complementary **Know-Your-Business (KYB)** checks for organizational customers and **Know-Your-Supplier (KYS)** diligence for our partners, forms a cornerstone of our robocall mitigation efforts. These processes ensure we thoroughly **identify, verify, and vet** all clients (and certain high-risk partners) before and after provisioning service, so that illegal robocallers are kept off our network. Key elements of Tru Voip's KYC and vetting protocols include:

- **Customer Identity Verification (KYC):** For every new customer, whether an individual or a business, Tru Voip performs rigorous identity verification. Individuals must provide valid government-issued photo identification and proof of current address. For business entities, we require official corporate documentation to establish the company's identity and good standing (e.g. articles of incorporation or formation, business registration certificates, or certificates of good standing from the state of incorporation). We collect the full legal name, physical address (no P.O. boxes), and contact information of the business and its principal owners or executives. These responsible parties are subject to personal identification checks as well. Tru Voip verifies all provided information through authoritative third-party sources. For example, we use identity verification services and government databases to confirm that personal IDs are authentic and match the individual, and we cross-check business EIN/tax ID numbers against official records to ensure they correspond to the registered business name. We also screen the names of customers and key principals against relevant watchlists, such as the U.S. Treasury's OFAC sanctions list and other law enforcement databases, to ensure no barred or high-risk persons are involved. Any discrepancy or red flag triggers enhanced due diligence – for instance, requests for additional documentation or explanations, or escalated review by our compliance team. Customers that cannot satisfactorily verify their identity or that present unacceptable risk profiles are rejected upfront.

- **Business Use Case and Intent (KYB):** In addition to verifying identity, Tru Voip vets each business customer's *intended use* of our voice services. We require a clear description of the customer's industry, business model, and specific use cases for our service (e.g. outbound sales call campaigns, appointment reminders, wholesale VoIP resale, call center operations, etc.). This information helps us assess the risk level and legitimacy of the customer's planned calling patterns. For example, a customer intending to run high-volume telemarketing or a predictive dialer will undergo closer scrutiny, including demonstrating compliance plans for consumer consent and opt-out management. Enterprise and wholesale clients must acknowledge our Acceptable Use Policy and explicitly agree not to use the service for any unlawful purposes. We incorporate "know-your-traffic" analysis – evaluating expected call volumes, destinations, and calling practices against industry benchmarks for that type of customer. If anything in the proposed use case suggests elevated risk (such as cold-call telemarketing to consumers, political polling campaigns, etc.), we may impose additional safeguards or monitoring requirements as a condition of service. In some cases, we will decline to provide certain high-risk services (for instance, auto-dialed outreach to wireless numbers without proven consent mechanisms) to ensure compliance. By knowing our customer's business and why they are using our network, Tru Voip can proactively prevent scenarios that might lead to illegal robocalls.
- **Acceptable Use Policy Adherence:** As part of onboarding, every customer must review and agree to Tru Voip's Acceptable Use Policy (AUP), which codifies the robocall and spam restrictions in detail. Our AUP contains explicit prohibitions on using Tru Voip services for illegal, fraudulent, or abusive communications, and reiterates requirements such as no caller ID spoofing, compliance with telemarketing laws, and cooperation with traceback requests. Customers provide written acknowledgment (or digital acceptance) of these terms, creating a contractual obligation to abide by them. Violations of the AUP are grounds for immediate suspension or termination of service. (See Section 11 for more on customer obligations under our AUP.) This step ensures each customer is fully informed of our zero-tolerance stance from the very start of the relationship.
- **Continuous Monitoring and Re-Vetting:** KYC does not end after initial signup – Tru Voip continuously monitors and periodically re-vets our customers. We maintain updated records of each customer's key contacts and business status, and we may request renewed documentation or identity proof if credentials expire or if there are significant account changes. Our compliance team keeps abreast of industry reports and traceback incidents; if an existing customer is ever implicated in illegal robocalling or is the subject of an FCC/FTC enforcement action, we immediately re-evaluate that customer's fitness to remain on our network. We also utilize automated tools that monitor customer accounts

for unusual behavior (see Section 7) – if a customer’s calling patterns change drastically or begin to resemble abusive robocalling, we initiate a compliance review of that customer. Additionally, Tru Voip subscribes to industry notification programs (e.g. regulatory alerts, traceback consortium notices) that might flag suspicious traffic originating from certain entities. If any such flags point to one of our customers, we investigate promptly. This ongoing vigilance helps catch any bad actors who might have passed initial vetting but later engage in prohibited activities.

- **Disqualification and Enforcement:** Tru Voip will deny service to any applicant that fails our vetting standards or that is found to have provided false information during onboarding. If a customer is approved but later violates our robocall policies or legal requirements, we will swiftly suspend and ultimately terminate the customer’s service (see Section 9 on enforcement). We also maintain an internal “watch list” of any customers or former customers who have been involved in robocall incidents or complaints. Such customers, if not outright terminated, are subject to heightened monitoring and may be required to implement corrective measures. Repeat offenders or those who show an unwillingness to comply are permanently barred from our network. Furthermore, Tru Voip will not onboard any customer or reseller that is known to have a history of robocall violations or enforcement actions by authorities. We conduct checks (for example, searching the FCC’s published lists of entities under robocall cease-and-desist orders or other enforcement notices) during onboarding to screen out such high-risk entities. By strictly enforcing disqualifications and leveraging industry intelligence, we reinforce our commitment that Tru Voip’s services cannot be used as a haven for illegal robocallers.

- **Know-Your-Supplier (KYS):** In our role as an intermediate provider, Tru Voip also vets the **upstream carriers and partners** that send traffic into our network. We only accept call traffic from reputable carriers or customers who have themselves certified compliance with robocall mitigation requirements. For instance, before we peer or exchange traffic with another provider, we verify that the entity is registered in the FCC’s Robocall Mitigation Database (as required for all voice providers) and has either implemented STIR/SHAKEN or filed a mitigation plan. We perform due diligence similar to KYC for our wholesale partners: checking corporate identity, industry reputation, and whether they have been subject to any FCC enforcement or traceback issues. Our contracts with interconnecting carriers include clauses requiring them to actively monitor and prevent illegal robocalls on their side and to cooperate with traceback investigations. If an upstream provider is uncooperative or is found to be a consistent source of illegal traffic, Tru Voip will cease accepting their traffic (see Section 8 on inbound mitigation). In summary, Tru Voip’s vetting protocols extend to all who use our network – customers and partners alike – ensuring a chain of trust and compliance.

7. Real-Time Call Monitoring and AI-Based Analytics

Tru Voip employs advanced real-time call monitoring systems and AI-driven analytics to detect and mitigate fraudulent or suspect calling activity **as it happens**. Our network is under continuous surveillance by automated algorithms that analyze call signaling and traffic patterns to flag anomalies characteristic of illegal robocalls or spam. This dynamic monitoring enables Tru Voip to identify problematic call campaigns early and take action in-flight, minimizing the potential for abuse. Key components of our real-time monitoring and analytics include:

- **Traffic Pattern Analysis:** We continuously analyze calling patterns on our network for indicators of robocall campaigns. Our systems monitor metrics such as call volumes, call durations, call answer rates, and calling distribution in real time. Unusual patterns trigger automatic alerts – for example, an extremely high volume of short-duration calls, rapid sequential dialing across many destination numbers, or bursts of calls to numbers in disparate area codes can all be signs of auto-dialer or war-dialing activity. Our platform knows the “normal” calling profile for each customer (based on their historical usage and stated use case) and uses statistical baselines to detect anomalies. If a particular source suddenly begins generating traffic far outside its normal pattern – say, hundreds of calls per minute when typically it makes a few calls per hour – our system will flag this deviation immediately for investigation or automatic mitigation. We leverage both internal algorithms and external data sources in this pattern analysis. The system can correlate observed calling behaviors with known robocall signatures (for instance, a surge of very short calls to many numbers often indicates a scam auto-dialer testing which numbers are active). When such patterns are identified, Tru Voip’s controls can automatically rate-limit, tag, or block the suspect calls (as detailed in Section 8).
- **Anomaly Detection with AI:** Tru Voip has invested in artificial intelligence and machine learning tools to enhance our fraud detection capabilities. Our AI models are trained on large datasets of voice traffic (including examples of confirmed illegal robocall campaigns and legitimate traffic) to recognize subtle indicators of illicit activity. These models evaluate multi-dimensional factors: not just volumes and rates, but also time-of-day distributions, call audio characteristics, interaction patterns, and historical behaviors. For example, an AI model may detect that a given calling campaign has an abnormal answer-to-hangup timing profile or that it uses pre-recorded audio identical to known scam robocalls. We utilize **voice fingerprinting** technology, which can compare audio streams of calls against a database of known scam recordings (such as IRS impersonation scams, etc.). If a match is found – i.e., the audio of an ongoing call matches a “fingerprint” of a

notorious robocall – the system can immediately mark that call as fraudulent. AI-driven **reputation scoring** is also applied to calling numbers: using both Tru Voip’s internal data and third-party reputation services, each originating number is assigned a risk score indicating likelihood of being a robocaller or spam source. Calls from numbers with poor reputations (for example, numbers that have accumulated consumer complaints or appear in industry scam number lists) are given heightened scrutiny or blocked. These AI and machine learning systems run in real time, meaning they can evaluate calls and make mitigation decisions in milliseconds as call setup occurs.

- **Do-Not-Originate (DNO) and Threat Intelligence Feeds:** Tru Voip actively leverages industry **DNO lists** and other threat intelligence to stay ahead of known scam operations. We subscribe to dynamic robocall threat intelligence feeds that provide up-to-the-minute information on bad actor caller IDs, suspicious IP addresses or SIP endpoints, and known robocall scams. For example, the USTelecom Industry Traceback Group and other industry bodies publish **Do-Not-Originate lists** of telephone numbers that should never originate traffic (such as inbound-only government or corporate numbers that fraudsters sometimes spoof). Tru Voip’s systems are configured to automatically block any call originating from a number on these DNO lists. If such a call attempt is detected, we reject it before it leaves (for outbound) or as it enters (for inbound) our network, and the event is logged for audit. We also utilize external data from traceback consortiums, telecom analytics firms, and public complaint databases to update our internal blacklist. This **internal blacklist** consists of numbers and SIP identifiers associated with illegal robocall campaigns. It is continually updated; any call matching an entry on the blacklist is automatically refused. Additionally, we ingest *reputation scores* from third-party analytics services which monitor global traffic patterns – if a calling number has been flagged as “spam likely” or abusive by multiple sources, our platform will either block the call or tag it with a warning for the callee. By integrating these threat intel feeds, Tru Voip benefits from collective industry knowledge to pre-emptively shut down calls that are very likely to be unlawful or harmful.

- **Real-Time Dashboard and NOC Oversight:** Tru Voip’s Network Operations Center (NOC) and compliance team have real-time visibility into network traffic through a specialized dashboard. This interface highlights key calling statistics and any alerts generated by our anomaly detection systems. The NOC staff is empowered to intervene manually if needed – for instance, if an alert shows a customer’s traffic pattern suddenly matching a robocall signature, the staff can initiate an immediate investigation or implement filters (like blocking a specific call type or number range). Our monitoring tools also allow drill-down to call records in real time, so suspicious call attempts can be traced and analyzed on the spot. The NOC works hand-in-hand with our AI systems: automated

algorithms handle the bulk of instantaneous decisions, while human analysts review flagged incidents for confirmation and further action. This combination of automation and human oversight ensures a rapid yet accurate response to emerging threats.

- **Internal Metrics and Tuning:** We collect extensive metrics on all the above monitoring activities, which feed back into improving our system. For example, we track how many calls were blocked or tagged as spam, false positive/negative rates of our AI detections, traceback requests handled, and other key performance indicators. A dedicated internal committee periodically reviews these metrics and the outcomes of mitigation actions (see Section 10 on Audit Logs) to adjust thresholds or rules for better efficacy. Our goal is to continuously refine the balance between aggressively stopping illegal calls and avoiding impact on legitimate traffic. We also stay abreast of new scam tactics and update our detection algorithms accordingly. In summary, Tru Voip's real-time monitoring and analytics create an intelligent, adaptive defense mechanism. By catching suspect calls in real time – using AI and data-driven insights – we significantly mitigate the risk of illegal robocalls traversing our network, enhancing overall network integrity and consumer protection.

8. Inbound and Outbound Robocall Mitigation Practices

Tru Voip employs rigorous mitigation practices for both **outbound** calls (calls originating from our customers or network) and **inbound** calls (calls coming into our network destined for our customers or transiting to other carriers). In both directions, our strategy is to **screen, score, quarantine, or block** suspicious traffic so that illegal or unwanted calls are stopped as early as possible. Below, we outline specific steps for outbound and inbound call mitigation.

Outbound Call Mitigation: Outbound traffic from Tru Voip's network is subject to multi-layered checks before and during call processing to ensure compliance and to intercept illegal calls:

- *Caller ID Authentication:* As described in Section 5, every outbound call is screened for valid caller ID and is signed with STIR/SHAKEN attestation when possible. Calls with unauthorized or invalid caller IDs are automatically blocked at origination. This prevents common spoofing-based scams from being launched through our system.
- *Pre-Call Vetting:* Our platform evaluates each outbound call attempt against the originating customer's profile and known behavior. If the call attempt falls outside expected parameters (e.g., a sudden mass dialing event from a customer that typically sends low volume, or calls to high-risk destinations), it may be diverted for further analysis. We also

check that the customer's account is in good standing and not subject to any compliance flags before allowing calls to proceed.

- *Realtime Traffic Monitoring:* During live call traffic (as detailed in Section 7), our real-time analytics watch for patterns indicative of robocalls. For instance, if an outbound traffic stream exhibits known markers of a robocall campaign – such as extremely high calls-per-second rates, a majority of calls being very short in duration, or concurrent calls to many different area codes – our system can automatically intercept or throttle those calls. Suspicious call attempts may be dropped before completion or shunted to a “mitigation queue” for closer inspection. Tru Voip's network can apply **rate limiting** on the fly: if a certain customer or trunk begins originating calls above a safe threshold, we temporarily cap the call rate to prevent a potential robocall barrage from flooding the network. This gives our team time to investigate while containing any potential harm.
- *STIR/SHAKEN Failure Handling:* If for any reason an outbound call cannot be fully authenticated with STIR/SHAKEN (for example, if a call's caller ID is not eligible for attestation A under our policy), we handle it according to predefined policies. In many cases, we will still allow the call but mark it appropriately – such calls might be sent with a lower attestation level and a “verification failed” indicator so that downstream carriers are aware of the risk. However, if the call is assessed as high risk (unauthenticated and matching other scam indicators), we may block it outright. Especially for international or gateway scenarios where STIR/SHAKEN isn't in end-to-end use, any outbound call lacking proper authentication is treated with extreme caution in our network.
- *Do-Not-Call (DNC) Compliance:* Tru Voip enforces strict compliance with Do-Not-Call rules and calling consent requirements for all outbound campaigns. We require that any outbound telemarketing or informational campaign run by our customers uses a scrubbed calling list that excludes numbers on the National Do Not Call Registry, as well as any internal do-not-call lists the customer maintains. Tru Voip provides tools (and APIs) to customers to aid with this compliance – for example, we enable customers to upload their DNC-suppressed lists into our platform, and our systems can automatically filter out calls to those numbers. We perform random audits of high-volume outbound customers to ensure they are honoring DNC obligations. Furthermore, for certain types of high-risk calls (like pre-recorded messages or predictive dialer calls to consumers), we implement additional safeguards. Tru Voip may require *opt-in verification* for these campaigns – for example, a customer might need to demonstrate to us that they have obtained prior express consent from the call recipients, as required under the TCPA for autodialed or pre-recorded telemarketing calls. If we are not satisfied that proper consent exists, we will not allow the campaign to proceed. Our enforcement policy is clear: any customer found to be

repeatedly violating telemarketing consent rules or DNC requirements will have their calling campaigns halted and may face account suspension or termination. By combining technical call analysis with proactive compliance checks (like DNC list enforcement and consent verification), our outbound mitigation ensures illegitimate or unlawful calls are blocked at the source, protecting end users and complying with regulations.

- *Enforcement of AUP in Outbound:* In cases where outbound traffic is detected that violates our Acceptable Use Policy (e.g., an illegal robocall campaign or spam calls), Tru Voip's compliance team is immediately engaged. We will typically suspend the customer's outbound calling capabilities while investigating. The customer is contacted and asked to provide an explanation or proof of compliance (such as evidence of consent for the calls in question). If the activity is confirmed to be illegal or against our terms – or if the customer fails to promptly remedy the issue – Tru Voip will terminate the offending traffic and possibly the service for that customer altogether. Our contracts and AUP give us full authority to suspend or terminate service without prior notice in order to protect the network and the public. This swift enforcement capability is a key part of outbound mitigation: it not only stops ongoing abusive calls but also acts as a deterrent to any customer considering violating our policies.

Inbound Call Mitigation: Tru Voip also applies diligent robocall mitigation measures to inbound calls – both those destined for our end-user customers (e.g., calls to DID's we host or to our hosted PBX clients) and those that transit our network as an intermediate provider. Our goal is to shield call recipients from known scam calls and to prevent Tru Voip from carrying unlawful traffic handed off from upstream sources. Inbound mitigation practices include:

- *STIR/SHAKEN Verification:* When an inbound call enters Tru Voip's network from another carrier or provider, we immediately check if the call carries a STIR/SHAKEN Identity header (i.e., if it was signed by the originating provider). If so, our systems perform cryptographic verification of the signature and evaluate the attestation level. Calls that fail verification – for example, if the digital signature is invalid or the signing certificate is untrusted – are marked as **suspect**. Depending on the context (and customer preferences), we may reject such calls outright or label them for the called party. In some cases, we will deliver the call but with an indicator (such as a "Spam Likely" caller ID prefix or a warning in our portal) to alert the end user that the call's authenticity is in doubt. By contrast, calls that pass STIR/SHAKEN verification (especially those with A or B attestation) are treated as lower-risk – though we still apply additional screening as described below.

- *Inbound Analytics and Blocking:* Even for inbound calls that have a valid STIR/SHAKEN signature or for calls coming from networks where STIR/SHAKEN isn't available (e.g., some international or TDM calls), Tru Voip applies multiple analytics layers to detect robocalls. We utilize the same AI-driven tools and threat intelligence described in Section 7 on inbound call attempts. For example, we compare the calling number against our internal and external **spam number lists** – if the Caller ID number is known to be used by robocallers or appears on a real-time industry scam list, our system can automatically block the call or divert it to a voicemail screening system. We also examine call signaling patterns (such as whether the call came through an unusual pathway or exhibits hallmarks of spoofing). In some cases, we deploy an interactive *CAPTCHA* or challenge for suspicious inbound calls – e.g., requiring the caller to press a digit or speak a response – to distinguish between automated dialers and legitimate human callers. Calls that fail the challenge are disconnected. Additionally, we maintain an **inbound threat score** for each call using third-party analytics: if a call's score exceeds a certain risk threshold (indicating a high probability of being spam/fraud), the call is intercepted and dropped or labeled accordingly. These measures help ensure that our end-user customers and PBX systems are protected from the bulk of mass robocalling attempts.
- *Do-Not-Originate & Blacklists:* As noted earlier, any inbound call purporting to be from a number on a Do-Not-Originate list (such as the IRS's main number, etc.) is automatically rejected by our ingress filters. We also block calls from invalid or unallocated numbers (for instance, if the Caller ID has an area code/exchange that is not assigned, or a number that fails format validity). Our internal blacklist of known scam sources (updated via industry feeds) is enforced at inbound gateways, preventing repeat offenders from attempting calls to our users. This proactive blocking stops many scam calls at our network border, never reaching the intended targets. All such blocked events are logged with details (calling number, timestamp, etc.) for auditing.
- *Caller Reputation Labeling:* In cases where we do not block an inbound call but have some suspicion about it, Tru Voip may employ **call labeling** to inform the recipient. For example, for calls delivered to our hosted PBX users, we can insert a prefix in the caller ID display like "[SPAM?]" or "[Scam Likely]" based on the reputation analysis. This allows the called party to decide whether to answer. Similarly, we can send calls to a quarantine (like straight to voicemail) if they are likely unwanted, based on customer settings. Our goal is to empower end users with information and options to avoid scam calls, in line with FCC encouragement of call blocking and labeling services.
- *Upstream Provider Controls:* As an intermediate carrier, Tru Voip also mitigates inbound traffic handed from other carriers to us for termination. We adhere to the FCC

requirement that we should not accept traffic from voice service providers who are not compliant with the Robocall Mitigation Database rules. In practice, Tru Voip refuses to carry inbound calls from any domestic carrier or VoIP provider that has failed to file a robocall mitigation certification with the FCC. We verify the status of new interconnect partners against the FCC database and periodically re-check existing ones. If an upstream provider is found unregistered or is later removed from the database, we will block their traffic until they comply. This policy helps close the gaps that illicit operators might exploit by hopping through non-compliant intermediaries. Additionally, if a normally trusted upstream peer suddenly sends an unusual spike of calls or a batch of obviously unlawful calls, our NOC is alerted and will intervene. We may temporarily block or throttle traffic from that source and reach out to the provider to address the issue (see Section 9 on Traceback Cooperation for escalation procedures). By policing our network boundaries in this way, Tru Voip helps prevent the propagation of illegal robocalls through the supply chain of carriers.

In summary, Tru Voip's inbound and outbound mitigation practices are designed to be complementary and exhaustive. Outbound controls stop our own customers from originating illegal robocalls, and inbound controls prevent external bad actors from reaching our customers or abusing our network as a transit point. These measures operate in real time and are continually updated to respond to new threats. Through a combination of technology, policy enforcement, and industry collaboration, Tru Voip effectively screens and neutralizes suspect call traffic in both directions, thereby upholding the integrity of our services.

9. Traceback Cooperation and Enforcement

Tru Voip is fully committed to cooperating with industry traceback efforts and law enforcement to identify and stop illegal robocallers, and we enforce strong consequences on any offending customers or partners. Our posture is one of active collaboration and swift action. The key aspects of our traceback cooperation and enforcement approach are:

- **Industry Traceback Group (ITG) Participation:** Tru Voip is an active participant in the Industry Traceback Group, the FCC-designated traceback consortium led by USTelecom. We have formally registered a designated point of contact for traceback requests in our Robocall Mitigation Database filing. Internally, we have a dedicated Traceback Response process: a team within our compliance department (headed by our regulatory and network security personnel) is on call to respond to any traceback inquiries. When Tru Voip receives a traceback request from the ITG or directly from enforcement

authorities, we treat it with top priority. Our team immediately queries our call detail records and other logs to trace the identified call to its source in our network. We are committed to responding *fully and within 24 hours* to all traceback requests from the FCC, law enforcement, or the industry consortium. In practice, we often respond much faster – frequently the same business day – given the urgency of stopping illegal campaigns. We provide all relevant information requested (e.g. originating customer/account, call timestamps, routing data) in a secure and confidential manner to the requesting parties. Tru Voip understands that cooperating with traceback requests is not just a legal obligation (per 47 CFR § 64.6305) but a critical industry responsibility to help pinpoint the origins of unlawful calls and remove bad actors from the network.

- **Cooperation with Law Enforcement:** Beyond the formal ITG tracebacks, Tru Voip cooperates fully with any law enforcement investigations into suspected illegal robocalling. If we receive subpoenas, National Security Letters, or other lawful requests for information about traffic on our network, we respond within the required timeframe and provide thorough, accurate data. We have established channels to work with the FCC’s Enforcement Bureau, the FTC, and state Attorneys General on robocall-related matters. For example, if law enforcement or regulatory agencies alert us to an ongoing scam operation using our services, we will immediately investigate and take remedial action (such as disabling the responsible accounts) while providing the agencies with the data they need. We also proactively reach out to law enforcement in cases where we detect a major illegal robocall campaign on our network – essentially volunteering information if it can help stop criminal activity. Tru Voip treats all such data sharing with appropriate confidentiality and in accordance with privacy laws and regulations. Unlawful robocalling is a widespread problem, and we recognize that only through close collaboration between industry and government can it be effectively combated. We are proud to contribute to these collaborative efforts.

- **Internal Enforcement and Customer Accountability:** On the enforcement side, Tru Voip takes decisive action to enforce our policies when a customer or partner is found to be involved in illegal robocalling. As described in Section 8, if our monitoring or a traceback indicates that a particular customer is originating unlawful calls, we will promptly suspend their ability to place calls while we investigate. Our compliance team will notify the customer and require an explanation. If it is determined that the customer indeed transmitted illegal robocalls or violated our terms (for instance, by conducting a campaign without proper consent or via spoofed numbers), we will terminate that customer’s service **immediately** for cause. Our Master Service Agreement and AUP give us the right to terminate service in the event of such violations, and we exercise that right to protect our network and the public. We also reserve the right to report egregious offenders

to law enforcement or regulators. In fact, if we disconnect a customer for robocall abuse, we retain documentation of the incident (call records, notices, etc.) and will, if appropriate, share relevant information with enforcement authorities to assist in any broader investigation. Similarly, if an *upstream provider* sending traffic to us fails to control illegal traffic, we escalate enforcement on that side: we will block the offending traffic, notify the provider, and if they do not promptly address the issue, we will sever the interconnection and report the behavior to the Industry Traceback Group and FCC. We cannot allow any partner to funnel illegal calls through our systems unchecked. These enforcement actions send a clear message that Tru Voip will not tolerate misuse of its services.

- **Transparency and Remediation:** As part of our enforcement philosophy, we strive to be transparent with industry and regulators. If Tru Voip itself ever were to become aware of a lapse in our own mitigation (for example, if some illegal calls escaped our controls), we would proactively reach out to the traceback consortium or FCC to report the issue and our corrective measures. Internally, every enforcement incident triggers a post-mortem analysis to see if there are ways to improve our processes or prevent a similar issue in the future. We maintain an internal watchlist (as mentioned in Section 6) of problematic customers or traffic sources, and enforcement history is factored into any future business decisions (e.g., we would not re-onboard a terminated customer without extraordinary reasons and assurances).

In essence, Tru Voip views cooperation with traceback and enforcement as more than just compliance – it is a core part of our corporate responsibility to the telecommunications ecosystem. We work hand-in-hand with the industry traceback initiatives and law enforcement agencies to root out illegal robocalling at every opportunity. Through prompt information sharing, robust internal enforcement, and a culture of accountability, Tru Voip helps ensure that those responsible for illegal robocalls are identified and dealt with, and that our own network remains hostile territory for any such malicious actors.

10. Data Retention and Audit Logs

Comprehensive data retention and logging are critical to Tru Voip’s robocall mitigation program. We maintain a robust audit infrastructure that records call events, mitigation actions, and relevant metadata, ensuring we have a complete evidentiary trail of our efforts to combat illegal robocalls. The following outlines our policies and systems for data retention and audit:

- **Call Detail Records (CDRs):** Tru Voip retains detailed call records for all calls handled by our network. These records include information such as timestamp,

origin/destination numbers, SIP identifiers, call duration, routing information, STIR/SHAKEN attestation (if applicable), and any disposition (e.g. completed, blocked, labeled). Our CDRs are stored in secure databases with redundant backups. We maintain CDRs for a minimum of 24 months (2 years), which exceeds many regulatory minimums, to ensure we can support investigations or compliance audits that may occur long after the call. This retention period is chosen to cover typical statutes of limitations for robocall-related enforcement actions, and we will preserve records even beyond this period if we know of an ongoing investigation (i.e., implementing a litigation hold).

- **Mitigation Action Logs:** In addition to basic call records, Tru Voip's systems generate logs for any mitigation or enforcement actions taken on calls. For example, if a call is blocked by our system (whether for caller ID spoofing, being on a blocklist, STIR/SHAKEN failure, etc.), a log entry is created noting the reason for the block, the triggering criteria, and the exact time and system that performed the block. Similarly, if a call is diverted to a CAPTCHA or marked as spam, that event is logged. These mitigation logs are correlated with the CDRs so we can reconstruct exactly what happened with any given call and why a certain action was taken. All customer-facing enforcement actions (such as rate-limiting or account suspension) are also logged along with any communications to the customer.
- **KYC and Compliance Records:** As part of our compliance data, Tru Voip securely retains all documentation related to customer identity verification (KYC) and onboarding vetting. This includes copies of IDs, business documents, completed AUP agreements, and notes from any compliance reviews or investigations. These records are kept for as long as the customer remains with us and for a defined period after termination (typically at least 2 years, aligning with our call data retention). In case of any regulatory audit, we can produce evidence of our diligence in vetting customers and enforcing our policies. Access to these sensitive records is restricted to authorized compliance personnel.
- **Audit Processes and Reviews:** Data retention alone is not enough; Tru Voip has instituted regular **audit processes** to review the data we collect. We run automated auditing scripts and reports to flag any anomalies in our mitigation systems. For example, we verify that all calls that should have been STIR/SHAKEN signed were indeed signed, and if any expected blocking rule did not trigger properly, it is caught in an audit. Our compliance team performs **quarterly audits** of random samples of call records and mitigation actions. They look for consistency with policy – e.g., checking that no illegal call slipped through unblocked, and conversely that no legitimate traffic was inadvertently blocked. If any discrepancies are found, they are documented and investigated, and remedial steps are taken (such as tuning a filter or retraining staff on a procedure). The

results of these audits are reported to Tru Voip's senior management and used to continuously improve our program.

- **Access Controls and Security:** All retained data and logs are protected with strong security controls. Access to detailed call logs and customer information is limited to authorized engineers and compliance officials on a need-to-know basis. We maintain audit trails of any access to sensitive data, to ensure there is accountability for how the information is used. Our storage systems are compliant with applicable privacy regulations, and we have measures in place to prevent unauthorized data exfiltration. In the event of any data relevant to a government investigation, we handle it in compliance with our privacy policy and legal requirements.
- **Support for Regulatory Audits:** Because we maintain extensive records, Tru Voip is well positioned to demonstrate compliance if the FCC (or another regulator) audits our robocall mitigation efforts. We can readily produce data showing our STIR/SHAKEN implementation status, the specific steps we have taken to avoid illegal traffic (including KYC processes as required by 47 CFR § 64.6305(d)(2)(ii)), and evidence of our rapid response to traceback requests. Our data retention practices ensure that even historical incidents (within the last two years or more) are documented. This comprehensive and reliable record of our fight against illegal robocalls provides confidence to regulators, partners, and our customers that Tru Voip is doing everything possible to uphold the law.

In summary, Tru Voip's data retention and audit log framework not only meets regulatory obligations but goes above and beyond to ensure transparency and continuous improvement. By keeping robust records of every facet of our robocall mitigation program – and regularly auditing those records – we create a feedback loop that strengthens our defenses. Our commitment to preserving evidence and analyzing it systematically is a key part of our compliance posture. It enables us to back up our certifications with hard data and to quickly correct any gaps that metrics or audits might reveal.

11. Customer Education and Obligations

Tru Voip believes that effective robocall mitigation is a shared responsibility between the service provider and the customer. While we implement strong network-level controls, we also ensure that our **customers understand their obligations** and are educated about lawful use of our services. To that end, we have established clear terms in our contracts (Master Service Agreement and Acceptable Use Policy) outlining customer responsibilities, and we actively communicate best practices to our clients. Below are the key customer obligations and our approach to customer education:

- **Contractual Commitments:** Every Tru Voip customer is bound by our **Master Services Agreement (MSA)** and **Acceptable Use Policy (AUP)**, which include strict provisions to prevent the usage of our services for illegal robocalling or any abusive behavior. Under these terms, customers agree to use Tru Voip services only for **lawful purposes** and in compliance with all applicable telemarketing and consumer protection laws. They must adhere to regulations such as the TCPA, CAN-SPAM Act (for texts), Telemarketing Sales Rule, and any analogous state laws. The AUP explicitly **prohibits caller ID spoofing or manipulation** – customers may not transmit false or misleading caller identification information, and may only use caller ID numbers that they are authorized to use. Customers are required to support and not undermine STIR/SHAKEN call authentication on their end, meaning they should not attempt to circumvent any call signing measures. Our terms also forbid any use of the service for fraudulent, deceptive, or harmful purposes. This includes a ban on auto-dialing or prerecorded calls to recipients who have not given consent where such consent is required by law.
- **Know-Your-Customer & Traceback Cooperation (Customer's Role):** Tru Voip's AUP contains a clause requiring customers to **cooperate with any traceback or fraud investigation**. If Tru Voip or an authority contacts a customer regarding suspected illegal calls originating through their account, the customer must respond promptly (generally within 24 hours) with complete and accurate information about the source of that traffic. If the customer is a reseller or carrier using our network, they must have their own processes to identify their end-users and are required to help trace those end-users if they generate spam or scam calls. This cooperation is not optional – it's a condition of service, and failure to comply can result in suspension. We also require that customers themselves **implement robocall mitigation practices** if they are in a position of originating significant traffic or sub-leasing services (the "know your end-user" concept). For example, if our customer is another voice provider or a call center platform, we expect them to vet *their* clients and have measures in place to prevent unlawful calls. Our AUP even specifies that if a customer is required by FCC rules to have its own robocall mitigation plan or certification (such as a downstream VoIP provider), they must do so as a condition of using our network. These requirements push responsibility down the chain and ensure alignment in anti-robocall efforts.
- **Telemarketing Compliance and Consent:** We emphasize to customers that if they use our service for any kind of telemarketing, mass dialing, or messaging, they **must follow all consent and opt-out rules**. Our AUP spells out that customers are solely responsible for obtaining any legally required **prior express consent** from call recipients, especially for autodialed or pre-recorded telemarketing calls, in accordance with the TCPA. They must also honor any **Do-Not-Call** requests or opt-outs – if a called party says "do not call me

again,” the customer must immediately add them to their internal DNC list and not contact them further. Unsolicited calls or texts to individuals without proper consent are strictly forbidden. We reinforce that predictive dialers and autodialers have specific legal restrictions (for instance, no autodialed calls to wireless numbers without consent, except for emergencies) and that violating these can incur heavy fines. Our customers also agree to **indemnify Tru Voip** for any fines or legal penalties incurred due to their unlawful calling practices, underscoring the importance of compliance on their part.

- **Prohibited Content and Activities:** Tru Voip’s policies also enumerate types of content and activities that are banned on our platform, which we convey to customers. This includes a prohibition on using our service for scams, fraudulent schemes, phishing attempts, impersonation of others without authorization, or transmitting any content that is illegal, harassing, or harmful. We highlight that even content which might be legal under certain free speech protections could violate our terms if it poses a risk (for example, we disallow traffic related to obvious scam offers, etc., to protect overall network reputation). By making these points clear in our agreements, customers are educated from the outset about what is not acceptable.
- **Customer Education Initiatives:** Simply having rules in fine print is not enough – Tru Voip actively educates our customers about these obligations. At service initiation, we provide new customers with a “Compliance Welcome Kit” that summarizes key rules: e.g., guidance on obtaining consent for calls, tips for managing opt-outs, how to use our DNC scrubbing tools, and explanation of STIR/SHAKEN and why it matters. We regularly update our customers via email newsletters or portal announcements about relevant regulatory changes (for instance, if the FCC issues new robocall mitigation requirements or if new industry best practices emerge). For customers who run call centers or high-volume operations, our account managers often hold a compliance briefing call to walk them through our expectations and the features we offer (like CAPTCHA for inbound calls or API hooks for checking numbers against DNC lists). We also point customers to FCC and FTC resources on robocall and telemarketing compliance for further reading. By being proactive in education, we aim to prevent inadvertent violations by customers who might simply be unaware of the rules.
- **Monitoring Customer Compliance:** In addition to initial education, Tru Voip monitors customer behavior to ensure they uphold their obligations. As described in prior sections, we perform random audits of high-volume callers for DNC compliance and we monitor traffic for signs of unlawful practices. If we notice a customer’s call patterns could be problematic (e.g., short calls that suggest pre-recorded messages without opt-outs), we will reach out to that customer to discuss what they are doing and remind them of the

rules. This open communication allows customers to correct course or seek guidance if needed. We much prefer helping a customer comply than having to enforce after a violation. Nonetheless, when willful or repeated violations occur, we do enforce as discussed – such as suspension or termination of service in serious cases.

- **Shared Commitment Clause:** Lastly, our customer communications stress that preventing robocalls is a shared commitment. We use language in our agreements and customer materials that by using our services, the customer **certifies** they too are taking measures to combat illegal calls. We find that most customers – especially legitimate businesses – share the goal of eliminating bad actors, as robocall scams hurt everyone's answer rates and trust in voice calls. Tru Voip fosters a partnership mentality: we provide the tools and oversight, and we expect customers to run their operations ethically and lawfully. This mutual commitment is essential for the long-term success of robocall mitigation efforts.

Through these combined efforts – clear contractual obligations, active education, available compliance tools, and diligent oversight – Tru Voip ensures that our customers know their responsibilities and are held to a high standard of conduct. By requiring compliance at the source (the customer) in addition to our network-level defenses, we create multiple layers of protection against illegal robocalls.

12. Point of Contact

For any inquiries regarding this Robocall Mitigation Plan or Tru Voip's robocall prevention practices, please contact:

David Cantwell

President - Tru Voip LLC

Email: regulatory@Tru-Voip.com

Phone: (317) 217-4100

PO Box 40821

Indianapolis, IN 46240, United States