

Robocall Mitigation Strategy for VirtualPBX.com, Inc. Utilizing 2600hz Kazoo and Bandwidth Services

☰ Tags	FCC Robocall
📅 Last Updated	@June 3, 2025

1. Executive Summary: Navigating FCC Mandates for Robocall Mitigation

The Federal Communications Commission (FCC) has intensified its efforts to combat illegal robocalls, imposing significant new obligations on all voice service providers. FCC Public Notice DA-24-73A1, released in early 2024, outlines expanded requirements for the Robocall Mitigation Database (RMD) and mandates universal filing, compelling providers like VirtualPBX.com, Inc. to demonstrate proactive and effective measures against unlawful call traffic.[1] The urgency of these regulatory changes necessitates a comprehensive and technically sound mitigation strategy.

A cornerstone of this strategy is the robust implementation and management of STIR/SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENS). For VirtualPBX.com, Inc., operating on the 2600hz Kazoo platform and utilizing Bandwidth as its primary carrier in a Bring Your Own Carrier (BYOC) model, this presents specific challenges and responsibilities. Notably, the upcoming **June 20, 2025, deadline** for providers to use their own STIR/SHAKEN certificates and determine call attestation levels underscores the need for immediate and strategic action.[2] VirtualPBX.com, Inc. is meeting this deadline by obtaining its own STIR/SHAKEN certificates and utilizing Bandwidth's hosted signing service. Bandwidth hosts these certificates and integrates with the VirtualPBX.com, Inc. platform to ensure correct call categorization, while VirtualPBX.com, Inc. retains full responsibility for determining call attestation levels.

This report details a multi-faceted robocall mitigation strategy tailored to VirtualPBX.com, Inc.'s operational environment. The core pillars of this strategy include:

- 1. Proactive STIR/SHAKEN Management:** Securing provider-owned STIR/SHAKEN certificates, utilizing Bandwidth's hosted signing service (with Bandwidth's platform integration for call categorization support) for implementation by the June 20, 2025 deadline, and accurately assigning call attestation levels.
- 2. Comprehensive "Know Your Customer" (KYC) Protocols:** Implementing rigorous customer vetting and ongoing monitoring processes, leveraging tools like Stripe Radar and detailed manual verification, to prevent the onboarding and misuse of services by malicious actors.
- 3. Advanced Traffic Monitoring and Anomaly Detection:** Leveraging Kazoo platform capabilities, Google BigQuery for CDR analysis, custom scripts for SIP anomaly detection, and an internal rules engine to identify and analyze suspicious calling patterns.
- 4. Effective Call Blocking Mechanisms:** Utilizing native Kazoo features, dialplan-level caller ID validation, SIP header analysis, IP reputation and geo-blocking, and integrating advanced solutions to block illegal robocalls at their source or within the network.
- 5. Diligent Traceback Cooperation:** Establishing clear procedures, including prompt service suspension for verified unlawful traffic and 12-month log retention, to respond to traceback requests from regulatory and law enforcement agencies within the mandated 24-hour timeframe.

The implementation of this strategy is not merely a compliance exercise; it is crucial for protecting the integrity of VirtualPBX.com, Inc.'s network, maintaining customer trust, and ensuring uninterrupted service delivery in an increasingly stringent regulatory landscape.

2. Understanding the Regulatory Landscape: FCC DA-24-73A1 and its Implications

The FCC's Public Notice DA-24-73A1 represents a significant tightening of robocall mitigation requirements, directly impacting all voice service providers, including VirtualPBX.com, Inc. Understanding these mandates is the first step toward ensuring compliance and avoiding severe penalties.

Expanded Robocall Mitigation Database (RMD) Filing Requirements

DA-24-73A1 established a universal obligation for *all* providers to submit or resubmit a comprehensive filing to the Robocall Mitigation Database by February 26, 2024.[1] This filing is more extensive than previous requirements and must include:

- A certification stating that all calls originated on their network are subject to a robocall mitigation program meeting FCC standards.
- The provider's STIR/SHAKEN implementation status (fully, partially, or not implemented).
- A detailed robocall mitigation plan outlining the specific "reasonable steps" the provider has taken to avoid the origination, carrying, or processing of illegal robocall traffic.
- The provider's business name, address, and other identifying information.
- The role(s) the provider plays in the call path (e.g., originating, intermediate).[1]

Critically, beginning May 28, 2024, voice service providers and intermediate providers are prohibited from accepting traffic from any non-gateway intermediate provider not listed in the RMD.[1] This mandate creates an interconnected compliance ecosystem, where VirtualPBX.com, Inc. must not only ensure its own RMD listing but also be mindful of the compliance status of its partners. The FCC has clearly signaled its intent to enforce these rules rigorously, adopting stricter RMD filing requirements to ensure widespread compliance and heightened awareness of provider responsibilities.[3] This indicates that submitted mitigation plans will likely face greater scrutiny.

Core Components of a Robocall Mitigation Program

The FCC mandates that a provider's robocall mitigation program must include "detailed practices that can reasonably be expected to significantly reduce" the origination or carrying of illegal robocalls.[1] It is not enough to simply have a plan; providers "must comply with the practices" their program dictates. The program is deemed insufficient if the provider "knowingly or through negligence" originates or carries unlawful robocall campaigns.[1] This language underscores that the FCC expects active, demonstrable implementation and enforcement of the documented plan, moving beyond a mere paper exercise.

A pivotal commitment within the mitigation program is the requirement to respond fully, within 24 hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. Providers must also cooperate with these entities in investigating and stopping illegal robocallers using their services.[1]

Consequences of Non-Compliance

The ramifications of failing to comply with these expanded RMD requirements are severe. Providers not listed in the RMD, or those removed due to non-compliance, will have their traffic blocked by other providers, effectively isolating them from the public switched telephone network.[1, 4] The FCC's Enforcement Bureau has already identified numerous voice service providers for potential removal from the RMD for failing to meet filing requirements, demonstrating a commitment to enforcement.[4] This makes robust compliance an existential concern for voice service providers.

The shift in FCC posture, from basic registration to demanding detailed, auditable mitigation plans and proactive verification of ecosystem partners, signals a significantly increased compliance burden. The February 26, 2024, deadline for RMD resubmission was a critical juncture, and the ongoing obligation to maintain an accurate and effective mitigation plan is paramount.

The following table summarizes the key requirements and deadlines from FCC DA-24-73A1 pertinent to VirtualPBX.com, Inc.:

Table 1: FCC DA-24-73A1: Key Requirements & Deadlines for VirtualPBX.com, Inc.

Requirement	Detailed Description (citing relevant FCC rules, e.g., 47 CFR § 64.6305)	Critical Deadline(s)	Implications for VirtualPBX.com, Inc.	Relevant Documents
Universal RMD Filing/Resubmission	All providers must submit/resubmit a filing to the RMD including certification of a mitigation program, STIR/SHAKEN status, detailed mitigation plan, business info, and role in call path. (47 CFR § 64.6305(d), (e), (f))	February 26, 2024 (Past)	Urgent: Verify filing status. If not filed/resubmitted, immediate action required. Ensure plan is comprehensive and accurate.	[1]
Prohibition on Accepting Traffic from Unlisted Non-Gateway IPs	Voice service providers and intermediate providers must refuse traffic from any non-gateway intermediate provider not listed in the RMD.	Beginning May 28, 2024 (Ongoing)	Must verify RMD status of upstream non-gateway intermediate providers. Risk of service disruption if partners are non-compliant.	[1]
Robocall Mitigation Program Standards	Program must describe specific "reasonable steps" taken to avoid illegal robocall traffic. Provider "must comply with the practices" and is accountable for negligence. (47 CFR § 64.6305(b))	Ongoing	Mitigation plan must be actively implemented, enforced, and auditable. Not just a document, but operational procedures.	[1]
Traceback Cooperation	Commit to respond fully within 24 hours to all traceback requests from FCC, law enforcement, and ITG, and cooperate in investigations. (47 CFR § 64.6305(b)(3))	Ongoing (24-hour response window per request)	Establish clear, efficient internal processes and designate a point of contact for rapid traceback response.	[1]
Stricter RMD Filing Requirements	FCC adopting new rules to further tighten filing requirements for the RMD to better ensure widespread compliance and heightened awareness.	Ongoing (as new rules are adopted, e.g., FCC-24-135)	Expect continued evolution of RMD requirements and increased scrutiny of filings. Maintain vigilance on FCC updates.	[3]

3. STIR/SHAKEN Implementation Strategy for VirtualPBX.com, Inc.

Effective STIR/SHAKEN implementation is central to any credible robocall mitigation strategy and is a key focus of FCC mandates. For VirtualPBX.com, Inc., leveraging the 2600hz Kazoo platform with Bandwidth as a primary carrier (BYOC model) requires a carefully considered approach to STIR/SHAKEN.

Understanding STIR/SHAKEN Fundamentals

STIR (Secure Telephone Identity Revisited) and SHAKEN (Signature-based Handling of Asserted information using toKENs) are protocols designed to combat illegal caller ID spoofing. They work by having the originating service provider (or a provider acting on their behalf) add a digital certificate to the Session Initiation Protocol (SIP) information used to initiate and route calls.[5, 6] This certificate, contained in a SIP Identity header, attests to the legitimacy of the calling number's use.

STIR/SHAKEN assigns an attestation level to each call, indicating the provider's confidence in the caller's right to use the presented caller ID:

- **A (Full) Attestation:** The highest level. The provider has authenticated its customer (Know Your Customer - KYC) and has verified that the customer is authorized to use the telephone number.[5, 7]
- **B (Partial) Attestation:** The provider has authenticated its customer, but has not verified that the customer is authorized to use the telephone number (e.g., a call from a PBX extension not directly assigned by the provider). [5, 7]
- **C (Gateway) Attestation:** The provider has authenticated the origin of the call (e.g., from a known gateway or another interconnected provider) but cannot authenticate the call source to the level of A or B attestation.[5, 7]

2600hz Kazoo Platform - STIR/SHAKEN Capabilities and Considerations

The 2600hz Kazoo platform's native STIR/SHAKEN capabilities are a critical factor for VirtualPBX.com, Inc. 2600hz has stated they are "in the process of updating our protocols with token based certifications per the new law".[8] However, a crucial point for a BYOC setup is their declaration that "Our implementation will only be certifiable with numbers purchased through 2600Hz. If you are a BYOC customer and acquire your numbers through a separate source, it is your responsibility to ensure your numbers are certified".[8] Since VirtualPBX.com, Inc. uses Bandwidth for its numbers, this means VirtualPBX.com, Inc. cannot rely solely on Kazoo's native STIR/SHAKEN for numbers provided by Bandwidth and must take direct responsibility for their certification and signing.

It is necessary to investigate Kazoo's ability to correctly handle and pass through SIP Identity headers if calls are signed by an external entity (such as Bandwidth's Hosted Signing Service or a dedicated third-party signing service). Kazoo documentation mentions that it "does include the data it finds in your account related to caller ID in its SIP packet, and sends it 'upstream' to the provider".[8] Furthermore, Kazoo's resource configuration allows for `custom_sip_headers` to be applied to calls outbound from 2600Hz to an endpoint.[9] These capabilities may provide the necessary mechanisms for inserting or passing through the STIR/SHAKEN Identity header. The lack of explicit documentation on how Kazoo handles Identity headers for calls already signed by the customer in a BYOC scenario [8] represents a technical gap that VirtualPBX.com, Inc. must address through testing and potential configuration adjustments. While there are community efforts around STIR/SHAKEN for older Kazoo versions like v4.3 [10], the strategy should focus on stable, supported solutions compatible with VirtualPBX.com, Inc.'s current Kazoo deployment.

Bandwidth as Primary Carrier - STIR/SHAKEN Services and Obligations

Presently, VirtualPBX.com, Inc. utilizes its primary carrier, Bandwidth, for STIR/SHAKEN signing of outbound calls, where Bandwidth applies its own certificates. Recognizing the evolving regulatory landscape, particularly the FCC's June 20, 2025 deadline, VirtualPBX.com, Inc. is actively implementing a compliant model. This involves VirtualPBX.com, Inc. securing its own STIR/SHAKEN certificates and utilizing Bandwidth's hosted signing service. Bandwidth hosts these VirtualPBX-owned certificates and integrates with the VirtualPBX.com, Inc. platform to support correct call categorization, while VirtualPBX.com, Inc. retains full responsibility for determining and assigning call attestation levels.

This approach addresses the FCC's Eighth Order concerning STIR/SHAKEN, which mandates an end to certain third-party authentication practices by **June 20, 2025**. [2] After this date, upstream providers like Bandwidth can no longer sign calls *on behalf* of their customers using *Bandwidth's own* STIR/SHAKEN certificate. Instead, the voice service provider originating the call (or the provider closest to the originator, like VirtualPBX.com, Inc. in this context) **must have its own Service Provider Code (SPC) token and its own STIR/SHAKEN certificate** issued based on that token. [2, 11] The provider must also determine and assign the attestation level for its outbound calls.

The strategy of using Bandwidth's "Hosted Signing Service" with VirtualPBX.com, Inc.'s own certificate is the definitive path for meeting the June 20, 2025 deadline. Under this model, VirtualPBX.com, Inc. loads its *own* certificate onto Bandwidth's platform. Bandwidth then performs the technical act of signing the calls using VirtualPBX.com, Inc.'s certificate. Crucially, VirtualPBX.com, Inc. remains responsible for determining and assigning the appropriate attestation level for each call.[11, 12] This ensures compliance with the FCC's requirements for provider-owned certificates and self-determined attestation.

While this is the confirmed strategy for the June 2025 deadline, VirtualPBX.com, Inc. may, for future consideration, evaluate implementing its own call signing infrastructure or engaging other specialized third-party STIR/SHAKEN signing services. If calls were to be signed *before* being passed to Bandwidth, Bandwidth has indicated it "will accept and transit the existing signature as is without needing to do anything more".[11]

Regardless of future considerations, the foundational steps for VirtualPBX.com, Inc. to participate in STIR/SHAKEN and meet the immediate deadline are:

1. **Obtain an Operating Company Number (OCN):** If not already possessed.
2. **File FCC Form 499-A:** Register with the FCC.[6, 11]
3. **Register with the STI-PA (Policy Administrator - iconectiv):** This is necessary to obtain an SPC (Service Provider Code) token.[6, 11, 13]
4. **Select an STI-CA (Certification Authority):** Use the SPC token to request and obtain a digital STIR/SHAKEN certificate from an approved STI-CA.[6, 11, 13]
5. **Configure Signing Solution:** Implement the Bandwidth Hosted Signing solution with VirtualPBX.com, Inc.'s own certificate.

The process of obtaining an OCN, SPC token, and certificates involves multiple entities and procedural steps, and therefore requires significant lead time. VirtualPBX.com, Inc. is actively managing this process to ensure timely compliance with the June 20, 2025, deadline.

Determining and Assigning Attestation Levels

As the originating service provider or the provider responsible for introducing calls into the network, VirtualPBX.com, Inc. is responsible for determining and assigning the correct attestation level (A, B, or C) for each outbound call.[2, 7] This decision cannot be delegated wholesale to Bandwidth and is a core responsibility of VirtualPBX.com, Inc. under the FCC's rules, especially for the June 20, 2025, deadline and beyond. Accurate attestation relies heavily on robust KYC processes (to validate the caller's identity) and telephone number validation procedures (to confirm the caller's right to use the number).

When utilizing Bandwidth's Hosted Signing Service (with VirtualPBX.com, Inc.'s own certificate), a technical mechanism, supported by Bandwidth's platform integration, is used for VirtualPBX.com, Inc. to signal the desired attestation level to Bandwidth for each call or for specific numbers. This typically involves API integration or configuration through Bandwidth's customer portal, facilitating the correct categorization of calls.[12] VirtualPBX.com, Inc. is ensuring its Kazoo platform effectively provides this signaling information to Bandwidth.

The combination of Kazoo's STIR/SHAKEN limitations for BYOC numbers and the evolving FCC regulations, particularly the June 20, 2025, deadline, mandates that VirtualPBX.com, Inc. take proactive and full ownership of its STIR/SHAKEN compliance. This includes owning its certificate, making its own attestation decisions, and ensuring the technical integration between Kazoo and Bandwidth's Hosted Signing service is sound and reliable for signaling attestation levels.

The following table outlines STIR/SHAKEN implementation, with Option 1 being the confirmed path for June 2025 compliance:

Table 2: STIR/SHAKEN Implementation Strategy for VirtualPBX (Kazoo & Bandwidth)

Aspect	Strategy for June 2025 Compliance: Bandwidth Hosted Signing (VirtualPBX Cert)	Future Considerations (Post-June 2025)	Key Actions for VirtualPBX (for June 2025 Compliance)	Relevant Documents
Certificate Ownership	VirtualPBX	VirtualPBX	Obtain OCN, File 499-A, Register with STI-PA for SPC token, Select STI-CA, Procure certificate.	[2, 6, 13]

Call Signing Location	Bandwidth Platform (using VirtualPBX's certificate)	Potential for Self-Signing (Kazoo-Integrated/Adjacent) or other Third-Party Signing Service.	Configure with Bandwidth for Hosted Signing using VirtualPBX certificate.	[8, 11, 12]
Attestation Assignment	VirtualPBX (signals to Bandwidth, supported by Bandwidth's platform integration for call categorization)	VirtualPBX (logic within Kazoo/adjunct or signaling to alternative service)	Develop robust KYC and number validation. Implement logic to determine attestation. Configure and test signaling mechanism to Bandwidth (e.g., API, portal configuration).	[2, 7, 12]
Kazoo Configuration	Configure to signal attestation to Bandwidth.	Potential modification of Kazoo to generate/insert SIP Identity header or integrate with local/alternative signing service.	Investigate and implement Kazoo's capabilities for signaling attestation to Bandwidth. Test thoroughly.	[8, 9]
Bandwidth Service	Hosted Signing Service (utilizing VirtualPBX's certificate)	Standard Trunking (if calls are pre-signed by VirtualPBX or another service).	Confirm with Bandwidth the exact technical requirements and integration points for attestation signaling when using their Hosted Signing service with VirtualPBX's certificate.	[11, 12]

4. Developing a Comprehensive Robocall Mitigation Program

While STIR/SHAKEN is a critical component, the FCC mandates a broader robocall mitigation program that encompasses several key areas. VirtualPBX.com, Inc. must develop and implement "reasonable steps" beyond call authentication to prevent illegal robocalls.[1]

A. Know Your Customer (KYC) and Onboarding Procedures

The FCC explicitly requires voice service providers to take "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence".[14, 15, 16] This is a foundational element of any robocall mitigation program.

VirtualPBX.com, Inc. maintains robust onboarding controls to verify customer legitimacy. These include:

- **Automated Fraud Risk Analysis:** All new accounts undergo automated fraud risk analysis using **Stripe Radar**. High-risk scores trigger a manual review process.
- **Manual KYC Vetting:** For customers flagged for manual review, or based on other risk criteria, VirtualPBX.com, Inc. performs enhanced due diligence, which may include collecting and verifying:
 - Government-issued ID for key individuals.
 - A live photo (selfie) of the individual holding the ID.
 - Address verification through utility bills or other accepted documents, if required.
- **Detailed Information Collection:** For all new customers, particularly commercial accounts, VirtualPBX.com, Inc. collects comprehensive information. This includes the legal business name, physical business address (P.O. boxes are insufficient for high-risk services), primary contact person(s) with verifiable contact details, state or country of incorporation, federal tax ID (or equivalent), and a clear description of the nature of the customer's business and intended use of voice services.[16, 17, 18]
- **Identity Verification:** Beyond automated checks, verification of the customer's identity is paramount. This can involve cross-referencing corporate formation records with relevant state agencies and using third-party services to verify physical addresses.[15]

- **Delayed Provisioning:** VoIP services are typically provisioned only after the satisfactory completion of KYC procedures, especially for new accounts or those presenting higher risk.
- **Risk Assessment:** A risk-based approach is applied throughout the customer lifecycle. Customers intending to use services for high-volume calling, employing auto-dialers or power dialers, or utilizing branded caller ID services that could potentially mask true identity undergo heightened scrutiny.[18] Commercial end-users, due to their potential for generating higher call volumes, may warrant a more stringent review process compared to individual residential users.[16]
- **Background Checks:** Compare customer information (company names, principals) against publicly available sanctions lists, FCC enforcement orders and public notices, and reports from state attorneys general or other consumer protection agencies. Bad actors frequently attempt to rebrand to evade detection, so identifying links to past illicit activities is crucial.[18]
- **Ongoing KYC and Risk Review:** KYC is not a one-time event. VirtualPBX.com, Inc. implements procedures for periodically refreshing customer data and audits customer behavior, including call patterns, at least **monthly** to ensure continued compliance with its Acceptable Use Policy (AUP) and to detect any emerging high-risk activities. This may include audit rights within service agreements and requiring recertification of compliance with acceptable use policies during contract renewals or service modifications.[16, 18]

B. Traffic Monitoring and Anomaly Detection

Continuous monitoring of network traffic for unusual or suspicious patterns is an explicit expectation under FCC guidelines.[16] VirtualPBX.com, Inc. must actively look for indicators of potential robocalling activity. This is achieved through a combination of platform capabilities, custom analytics, and an internal rules engine.

Leveraging Kazoo Platform Capabilities and Custom Analytics:

- **Call Detail Records (CDRs) Logging and Analysis:** All Call Detail Records (CDRs) generated by the 2600hz Kazoo platform are logged in **Google BigQuery**. This centralized repository allows for sophisticated analysis and reporting. CDRs include fields such as calling and called numbers, call duration (`billing_seconds`), hangup causes, call direction, and unique call identifiers.[19] Kazoo's API also allows for direct filtering and paginated retrieval of CDRs.
- **Scheduled BigQuery Analytics:** VirtualPBX.com, Inc. utilizes scheduled queries in Google BigQuery to proactively detect outliers in call behavior across accounts and originating IP addresses. This helps identify unusual call volumes, durations, and completion rates that may indicate robocalling.
- **Short Call Pattern Detection:** The system specifically flags accounts exhibiting a high volume of calls with very short durations. Such patterns are strong indicators of robocalling or call-blasting activities and trigger a manual review of the account.
- **Kazoo-Specific CDR Properties:** Properties like `resource_type` (e.g., 'offnet-origination', 'offnet-termination') within Kazoo CDRs are used to help identify the source and path of traffic, which is vital for pinpointing problematic call origins.[19]
- **Internal Rules Engine:** An internal rules engine is employed for threshold-based alerting and, if necessary, automatic throttling of call traffic from accounts that exceed predefined legitimate usage patterns or exhibit suspicious behavior.
- **SIP Anomaly Detection:** Custom scripts are run periodically to perform **SIP header inspection** to detect common spoofing patterns and to identify other SIP anomalies, such as malformed packets or the use of invalid codecs or call profiles.
- **Historical Fraud Detection Efforts:** 2600hz has previously discussed initiatives related to detecting and managing VoIP fraud, including aspects of call monitoring [20, 21], indicating a foundational awareness within the platform's development history that VirtualPBX.com, Inc. builds upon.

Complementary Role of Bandwidth:

Bandwidth, as an upstream carrier, also performs its own traffic analysis. They report monitoring metrics such as Minutes of Use (MOUs), call durations, and Automatic Number Identification (ANI) validation for anomalies, and will block calls exhibiting clear issues.[17] VirtualPBX.com, Inc. should understand these upstream efforts and ensure its own monitoring complements them, providing a deeper view into traffic originating from its direct customers.

Anomaly Detection Techniques (General):

Beyond the specific tools mentioned, VirtualPBX.com, Inc.'s monitoring aims to detect common indicators of robocalling:

- Unusually high call volumes from a single source or account, especially sudden bursts of traffic in short timeframes or significant deviations from established traffic patterns.[16, 22]
- A high percentage of short-duration calls.
- Low call completion rates.
- Unusual calling patterns, such as sequential dialing or calls to a large number of disparate geographic locations in a short period.[16, 23]
- Network anomaly detection principles involve establishing a baseline of normal network behavior using historical data and statistical analysis. When current traffic patterns significantly deviate from this baseline, an anomaly is flagged.[22]

Third-Party Analytics and Monitoring Tools (Current and Future Consideration):

VirtualPBX.com, Inc. currently utilizes

Google Cloud (BigQuery) for extensive call detail analysis and alerting. To further augment native and custom capabilities, VirtualPBX.com, Inc. will continue to evaluate and consider integrating specialized third-party services as the threat landscape evolves. Companies like YouMail Protective Services [24, 25], Ribbon Communications (Call Trust®) [26], and TransNexus (ClearIP, NexOSS) [23] offer advanced solutions including real-time reputation scoring, dynamic traffic analysis, and identification of calls from DNO lists or known high-risk sources. Integration of such services with the Kazoo platform would likely involve leveraging Kazoo's API capabilities, such as the Pivot application for real-time callflow modification based on external HTTP lookups [27], or custom development using Kazoo's SDKs.[28, 29]

C. Call Blocking and Filtering Mechanisms

An effective mitigation program must include robust mechanisms to block or filter illegal robocalls. VirtualPBX.com, Inc. employs a multi-layered approach:

Kazoo Platform and Network-Edge Blocking Features:

- **Rate Limiting:** To proactively manage call volumes and prevent abuse, VirtualPBX.com, Inc. currently employs specific technical controls at the platform level, such as utilizing FreeSWITCH's built-in `limit` module to enforce restrictions on maximum concurrent calls and calls per second (CPS) for all customer accounts.
- **Caller ID Validation:** As a direct measure against spoofing, VirtualPBX.com, Inc. implements caller ID validation where calls presenting with malformed or clearly suspicious caller ID information are proactively rejected at the Kazoo dialplan level.
- **IP Reputation & Geo Blocking:** IPs originating from high-risk geographies and those listed on known spam/abuse databases are automatically blocked at the network edge, preventing traffic from these sources from reaching the Kazoo platform.
- **Native Blocklist/Blacklist:** The Kazoo platform, through its Monster UI, offers a blocklist feature that allows users to filter unwanted *inbound* calls based on specific numbers or by blocking all calls identified as "Anonymous".[30] The documentation notes that this feature shares backend data with the Callflows application [30], implying some level of integration.

- **Blacklists API:** Kazoo provides a REST API (`/v2/accounts/{ACCOUNT_ID}/blacklists/{BLACKLIST_ID}`) for programmatic management of blacklists.[31] This API allows for creating, fetching, modifying, and deleting lists of numbers to be blocked.
- While the available documentation for the basic Blacklists API [31] and Monster UI blocklist [30] does not explicitly detail support for wildcard/pattern matching for *outbound* blocking or dynamic blocking based on STIR/SHAKEN attestation levels or reputation feeds, Kazoo's callflow engine does support regex (regular expressions) for pattern matching in call routing.[32] This underlying capability suggests that more sophisticated blocking logic for outbound calls could potentially be implemented through custom callflow configurations or by extending existing modules, though this would require further investigation and possibly development.

FCC Mandated Blocking:

- **Do-Not-Originate (DNO) Lists:** The FCC now requires *all* domestic voice service providers to block calls based on a reasonable DNO list.[33] VirtualPBX.com, Inc. will incorporate a DNO list lookup and blocking mechanism into its call processing.
- **Blocking Based on Reasonable Analytics:** Providers are required to block calls based on reasonable analytics. When such calls are blocked on IP networks, the provider must return SIP code 603+ (Decline / Blocked by an upstream provider) to notify the caller of the block.[33] This necessitates intelligent blocking capabilities beyond static lists and correct SIP signaling.

Third-Party Blocking Solutions (Current and Future Consideration):

VirtualPBX.com, Inc. leverages

Bandwidth for call transport, and Bandwidth may perform its own blocking of egregious traffic at its network edge. Many of the same third-party services that offer analytics also provide advanced blocking capabilities, which VirtualPBX.com, Inc. will continue to evaluate:

- **YouMail:** Offers real-time robocall blocking via API, leveraging its extensive threat database and reputation scores.[24]
- **Ribbon Communications:** Its Call Trust® portfolio includes tools to identify potentially illegal robocalls, assess risk, and block calls as required, often using reputation scoring queried via SIP or REST API.[26]
- **TransNexus:** Provides comprehensive blacklisting options (based on calling numbers, prefixes, originating SPIDs/OCNs, geographic locations, IP addresses, SIP user agents) and can screen calls against DNO lists or for high-risk numbers. Calls can be blocked or diverted (e.g., to a CAPTCHA gateway).[23]

Integration with Kazoo for Advanced Blocking:

To implement DNO list blocking, SIP 603+ responses, and to integrate third-party analytics/blocking services for outbound calls, VirtualPBX.com, Inc. will likely need to customize its Kazoo callflows. Kazoo's Pivot application, which allows callflows to make external HTTP requests to third-party servers for call treatment instructions [27], is a key enabler for such integrations. This would allow Kazoo to query an external analytics engine or DNO list provider in real-time and then apply blocking or routing logic based on the response.

D. Traceback Cooperation and Response Protocol

Prompt and effective cooperation with traceback requests is a non-negotiable FCC mandate.[1] The TRACED Act empowers the Industry Traceback Group (ITG), managed by USTelecom, to trace illegal robocalls back to their point of origin.

FCC Mandate and Internal Procedures:

- VirtualPBX.com, Inc. must commit to responding fully within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the ITG.[1]
- To meet this tight deadline, it is essential to dedicate sufficient internal resources and designate a single, clearly identified point of contact responsible for handling these requests.[16, 34] This contact must be knowledgeable and empowered to gather the necessary information quickly.

- Internal procedures are documented, outlining the steps for receiving a request, querying relevant systems (primarily Kazoo CDRs via BigQuery), compiling the response, and submitting it within the 24-hour window.
- If an investigation based on a traceback request or internal monitoring verifies unlawful traffic originating from a customer:
 - Services for the offending customer are **suspended immediately**.
 - The customer is notified of the suspension and the AUP violation.
 - Depending on the severity and history, the customer's services may be **terminated**.
- VirtualPBX.com, Inc. maintains call detail records and other relevant logs for **at least 12 months** to ensure full compliance with traceback requests and other investigative needs.

Utilizing Kazoo Data for Tracebacks:

- **CDRs:** Kazoo's CDRs, stored and analyzed in Google BigQuery, are the primary source of information for tracebacks. They contain essential details such as the unique `callId`, calling and called numbers, precise timestamps (including timezone information, which is critical), call duration, and potentially information about the path the call took through the network.[19] Efficient access to and querying of CDR data is vital.
- **Call Recordings:** If call recording is enabled for relevant services (and in compliance with all applicable laws regarding consent), recordings can provide additional evidence, such as the content of an illegal robocall message.[35] Kazoo's API allows for fetching specific recording documents and media.

Cooperation with Bandwidth:

Bandwidth, as an established carrier, has its own systems and processes for managing law enforcement inquiries and cooperating with ITG traceback efforts.[17, 36] If a traceback request involves a call that traversed both VirtualPBX.com, Inc.'s and Bandwidth's networks, coordinated responses may be necessary. VirtualPBX.com, Inc. should understand Bandwidth's procedures and ensure its own responses provide clear information about the segment of the call path it handled.

Information Required for Traceback:

Traceback requests typically require specific data points to be effective. These include the date, time (with timezone), and duration of the suspicious call(s); the calling and called telephone numbers; and, if available, an audio recording or transcript of the robocaller's message.[36] Maintaining accurate and easily retrievable records is therefore essential.

E. Acceptable Use Policy (AUP) Enforcement

A clear and consistently enforced Acceptable Use Policy (AUP) is a fundamental part of preventing network abuse.

- **Requirement:** VirtualPBX.com, Inc. maintains an AUP that explicitly prohibits customers from using its services to originate illegal robocalls or engage in other unlawful calling activities.[16] This AUP is part of the service agreement with all customers.
- **Alignment with Upstream Policies:** VirtualPBX.com, Inc.'s AUP is designed to align with, and be at least as stringent as, the AUP of its primary carrier, Bandwidth. Bandwidth's policies (which incorporate those of Voxbone, acquired by Bandwidth) prohibit the unlawful use of their services.[17, 37]
- **Customer Communication and Enforcement:** The AUP is clearly communicated to all customers at onboarding and is readily accessible. More importantly, VirtualPBX.com, Inc. has procedures in place to investigate reported or suspected AUP violations (identified through monitoring or complaints) and take appropriate action, which includes warnings, service suspension, or termination for customers found to be originating illegal robocalls, as detailed in Section 4.D.

Implementing these multifaceted program components requires a layered security approach. No single tool or process is sufficient. The open nature and API-driven architecture of the Kazoo platform [19, 27, 28, 29, 31, 32] provide significant flexibility for VirtualPBX.com, Inc. to integrate advanced mitigation tools and customize workflows.

However, this flexibility also implies a responsibility to undertake the necessary development or integration work, as comprehensive, out-of-the-box solutions for all advanced mitigation techniques may not be readily available. The 24-hour traceback response window further emphasizes the need for readily accessible data from Kazoo (primarily CDRs via BigQuery [19]) and highly efficient internal processes. Specific technical mandates, such as DNO list implementation and the use of SIP code 603+ for analytics-based blocking [33], will require precise configuration within Kazoo's call processing logic, likely through its callflow system.

The following table outlines the core components of the robocall mitigation program, reflecting current practices and planned enhancements:

Table 3: VirtualPBX Robocall Mitigation Program Components

Mitigation Area	FCC Requirement/Best Practice	Key VirtualPBX Tools/Practices (Kazoo, Custom, Third-Party)	Bandwidth Support/Interaction	Future Enhancement/Consideration	Relevant Documents
Know Your Customer (KYC)	Affirmative, effective measures to prevent new/renewing customers from originating illegal calls. Detailed vetting. [14, 15]	Stripe Radar for automated risk scoring; Manual vetting (Gov ID, selfie, address verification); Detailed info collection; Delayed provisioning; Monthly AUP compliance/behavior audits.	Bandwidth has its own KYC for direct customers; may provide guidance on best practices. [17]	Continued refinement of risk scoring; Enhanced background checks for very high-risk profiles.	[16, 18]
Traffic Monitoring & Anomaly Detection	Monitor network for suspicious patterns; examine CDRs. [16]	Google BigQuery for CDR logging & scheduled outlier detection; Short call pattern flagging; Internal rules engine for threshold alerts/throttling; Custom scripts for SIP header/anomaly detection.	Bandwidth monitors its network traffic for anomalies. [17]	Integration of real-time third-party reputation feeds (e.g., YouMail [24], Ribbon [26], TransNexus [23]) via Kazoo Pivot [27] for dynamic scoring.	[19, 22, 23, 24, 26, 27]
Call Blocking & Filtering	Block based on reasonable DNO list; use SIP 603+ for analytics-based IP blocks. [33]	FreeSWITCH limit module for rate limiting; Dialplan-level rejection of malformed/suspicious CIDs; IP reputation & geo-blocking at network edge; Kazoo blocklists/Blacklist API.	Bandwidth may block egregious traffic at its network edge.	Full DNO list integration with Kazoo callflows; Automated SIP 603+ responses for analytics-based blocks; Dynamic blocking based on integrated third-party reputation feeds.	[23, 26, 30, 31, 32, 33]
Traceback Cooperation	Respond fully within 24 hours to FCC, law enforcement, ITG. [1]	Designated contact; Documented 24hr response protocol; CDRs via BigQuery; Immediate service suspension/termination for verified abuse; 12-month log retention.	Bandwidth has established traceback cooperation processes. [17, 36]	Streamline data extraction further; Regular drills of traceback response.	[1, 16, 19, 34, 35, 36]
Acceptable Use Policy	Have and enforce AUP prohibiting	Clearly communicated AUP; Procedures for	Bandwidth AUP applies to services	Regular AUP review and updates based on evolving	[38]

(AUP) Enforcement	illegal robocalling. [16]	investigation and enforcement (warnings, suspension, termination).	VirtualPBX procures. [17, 37]	threats and regulations.	
------------------------------	---------------------------	--	-------------------------------	--------------------------	--

5. Robocall Mitigation Database (RMD) Filing and Ongoing Compliance for VirtualPBX.com, Inc.

Accurate and timely filing in the FCC's Robocall Mitigation Database (RMD) is a critical compliance obligation. The RMD serves as a central repository where voice service providers attest to their robocall mitigation efforts and STIR/SHAKEN implementation status.

Filing Process Overview

As mandated by FCC Public Notice DA-24-73A1, all voice service providers, including those with existing filings, were required to submit a new or updated filing to the RMD by **February 26, 2024**.^[1] If VirtualPBX.com, Inc. has not completed this updated filing, it must be addressed as an urgent priority. The RMD submission portal remains open for new and updated filings.^[1]

The RMD filing must comprehensively include:

1. **Certification of Robocall Mitigation Program:** A formal attestation that the provider has implemented and is adhering to a robocall mitigation program designed to prevent the origination of illegal robocalls.
2. **STIR/SHAKEN Implementation Status:** A declaration of whether the provider has fully implemented STIR/SHAKEN, partially implemented it, or has not yet implemented it on the IP portions of its network. This status should reflect the plan to use Bandwidth's Hosted Signing with VirtualPBX's own certificate by June 20, 2025.
3. **Detailed Robocall Mitigation Plan:** The actual plan document that describes the specific "reasonable steps" the provider has taken to avoid the origination, carrying, or processing of illegal robocall traffic. This plan should align with the components detailed in Section 4 of this report.
4. **Identifying Information:** The provider's legal business name, primary address, other relevant contact information, OCN, FCC 499 Filer ID, and FRN.
5. **Role(s) in Call Path:** A description of the roles the provider plays in the call ecosystem (e.g., originating service provider, intermediate provider).^[1]
6. **Company Ownership and Management Disclosure:** Information regarding company principals, parent companies, subsidiaries/affiliates, and corporate jurisdiction as required by FCC ¶46 of the Sixth Caller ID Authentication Report and Order (FCC 23-18).

Key Company Information for RMD Filing

In compliance with FCC requirements, including Paragraph 46 of the Sixth Caller ID Authentication Report and Order (FCC 23-18), the following company information is pertinent for the RMD filing:

- **Provider Name:** VirtualPBX, Inc.
- **FCC 499 Filer ID:** [Enter VirtualPBX, Inc. Filer ID here]
- **FRN (FCC Registration Number):** [Enter VirtualPBX, Inc. FRN here]
- **Company Principals:**
 - Paul Hammond, CEO — exercises operational control
 - Lon Baker, COO — exercises operational control
 - Luis Garcia, CTO — responsible for technical operations
- **Parent Company:** [Specify if VirtualPBX, Inc. has a Parent Company, or state "None"]

- **Subsidiaries/Affiliates:**
 - [Subsidiary Name, if any] – [Brief description of services or relationship]
 - [Affiliate Name, if any] – [Brief description of services or relationship]
 - (If none, state "None")
- **Corporate Jurisdiction:** Incorporated in California, United States.
- **Point of Contact for Robocall Mitigation:**
 - Name: [Full Name of Designated Contact]
 - Title: [Title of Designated Contact]
 - Email: [Email of Designated Contact]
 - Phone: [Phone Number of Designated Contact]

(This information should be kept current and updated in the RMD as necessary.)

Contents of the Robocall Mitigation Plan (for RMD submission)

The robocall mitigation plan submitted to the RMD is a cornerstone of the filing. It must be a detailed, factual representation of VirtualPBX.com, Inc.'s actual practices, not a generic template. This plan should clearly articulate:

- The specific KYC and customer vetting procedures implemented to prevent new and renewing customers from originating illegal traffic.[15, 16]
- The methods used for traffic monitoring and anomaly detection, including how CDRs and other data sources are analyzed.[1, 16]
- The call blocking and filtering mechanisms in place, including any use of DNO lists, analytics-based blocking, and third-party solutions.
- A definitive commitment to cooperate with traceback requests from the FCC, law enforcement, and the ITG, and to respond fully within 24 hours.[1]
- Details on telephone number validation practices to ensure customers have the right to use the numbers they present as caller ID.[16]
- Any other "reasonable steps" taken that contribute to mitigating illegal robocalls.

The level of detail is crucial; the FCC expects a description of "specific 'reasonable steps'".[1] Vague or overly general statements will likely be deemed insufficient and could jeopardize the validity of the RMD filing.

Maintaining and Updating the RMD Filing

The RMD filing is not a static, one-time submission. It must be treated as a living document that accurately reflects VirtualPBX.com, Inc.'s current mitigation efforts and STIR/SHAKEN status. Providers are obligated to amend their RMD filing if there are material changes to the information previously submitted. This includes, but is not limited to:

- Changes in STIR/SHAKEN implementation level (e.g., moving from partial to full implementation, or clarifying the use of hosted signing with own certificate).
- Significant modifications to the robocall mitigation program (e.g., adoption of new analytics tools, changes in KYC procedures).
- Changes in key contact information, company principals, or corporate structure.

Failure to maintain an accurate and up-to-date RMD filing can lead to serious consequences. The FCC has the authority to remove providers from the RMD for non-compliance, inaccurate filings, or if their mitigation efforts are found to be ineffective.[4] Removal from the RMD would result in other providers blocking traffic from VirtualPBX.com, Inc.

Internal Audit and Review Processes

To ensure ongoing compliance and the effectiveness of the mitigation program, VirtualPBX.com, Inc. should establish regular internal audit and review processes. These processes should:

- Periodically assess the efficacy of each component of the robocall mitigation program.
- Verify that the practices described in the RMD filing accurately reflect current operations.
- Review traceback response performance to ensure adherence to the 24-hour deadline.
- Maintain thorough documentation of all mitigation activities. This includes records of customer vetting, traffic analysis reports, details of blocked calls, traceback request logs and responses, and any updates made to the mitigation plan or STIR/SHAKEN implementation. Such documentation is invaluable in the event of an FCC inquiry or audit.

The RMD filing is a formal declaration to the FCC and the industry of a provider's commitment to fighting illegal robocalls. Its accuracy, completeness, and the underlying reality of the mitigation efforts it describes are paramount.

The following checklist can guide VirtualPBX.com, Inc. in preparing and maintaining its RMD filing:

Table 4: RMD Filing Checklist for VirtualPBX.com, Inc.

RMD Section/Requirement	Information to Provide	Internal Data Source/Documentation at VirtualPBX	Responsible Party/Department	Snippet Reference
Certification of Mitigation Program	Formal statement certifying adherence to a compliant mitigation program.	Signed attestation by authorized officer.	Legal/Compliance	[1]
STIR/SHAKEN Implementation Status	Current status: e.g., "Partially Implemented - Utilizing upstream provider for signing. Actively procuring own SPC token and certificate to utilize Bandwidth's Hosted Signing service by June 20, 2025."	STIR/SHAKEN project plan; Technical architecture diagrams; Vendor confirmations (e.g., Bandwidth); STI-PA/STI-CA application status.	Engineering/Technical Operations	[1]
Robocall Mitigation Plan Document	Detailed description of KYC, traffic monitoring, call blocking, traceback cooperation, DNO list usage, number validation, etc.	The comprehensive plan developed based on Section 4 of this report.	Compliance/Operations	[1, 16]
Business Identifying Information (Core)	Legal Name, DBA(s), Primary Address, OCN.	Corporate records; FCC registration details.	Legal/Administration	[1]
FCC Identifiers	FCC 499 Filer ID, FRN.	FCC filings and registration documents.	Legal/Compliance	-
Company Structure & Ownership	Principals exercising operational/technical control, Parent Company (if any), Subsidiaries/Affiliates (if any), Corporate Jurisdiction. (Ref: FCC 23-18, ¶46)	Corporate legal records, Organizational charts.	Legal/Compliance	-
Role(s) in Call Path	Specify if Originating Service Provider, Intermediate Provider, Gateway Provider, etc. (as applicable).	Network architecture documentation; Service descriptions.	Technical Operations/Product Management	[1]
Traceback Contact Information	Name, title, email, phone number of the designated	Internal personnel records; Traceback protocol document.	Designated Traceback Contact/Operations	[1]

	individual for traceback requests.			
Commitment to Block Illegal Traffic	Statement confirming commitment to not knowingly carry or process illegal robocalls.	Part of the mitigation plan text.	Legal/Compliance	[1]
Verification of Plan Effectiveness	Description of how the provider monitors and ensures the plan remains effective.	Internal audit procedures; Performance metrics.	Compliance/Operations	[1]

6. Recommendations and Action Plan

To effectively address the FCC's robocall mitigation mandates and protect its network, VirtualPBX.com, Inc. should implement the following prioritized action plan. This plan integrates the requirements of DA-24-73A1, the capabilities of the 2600hz Kazoo platform, and the services offered by Bandwidth, focusing on meeting the June 20, 2025 STIR/SHAKEN deadline using Bandwidth's Hosted Signing with VirtualPBX's own certificate.

Immediate Actions (Urgent - Next 30-60 days)

1. Robocall Mitigation Database (RMD) Filing:

- **Action:** If the comprehensive RMD filing due February 26, 2024, has not been completed or needs updating based on DA-24-73A1, prepare and submit it immediately. This submission must include a detailed robocall mitigation plan and all required company information as outlined in this report.[1]
- **Responsibility:** Compliance Lead, Technical Lead, Legal.

2. STIR/SHAKEN Foundational Steps (for own certificate):

- **Action:** Confirm current OCN (Operating Company Number) status and ensure FCC Form 499-A is on file and accurate. Initiate applications if missing.[6, 11]
- **Action:** Begin the registration process with the STI-PA (iconectiv) to obtain an SPC (Service Provider Code) token.[6, 13]
- **Action:** Research and select an approved STI-CA (Certification Authority) and initiate the process for procuring a STIR/SHAKEN digital certificate using the SPC token.[6, 13]
- **Responsibility:** Technical Lead, Compliance Lead.

3. Traceback Point of Contact Designation:

- **Action:** Formally designate and internally (and if required, externally via RMD filing) communicate the single point of contact responsible for receiving and responding to traceback requests within the 24-hour FCC mandate.[1, 34]
- **Responsibility:** Operations Lead, Compliance Lead.

4. Review Bandwidth Acceptable Use Policy (AUP) and Customer Agreements:

- **Action:** Review VirtualPBX.com, Inc.'s customer service agreements and AUP to ensure they are consistent with Bandwidth's AUP [17, 37] and explicitly prohibit illegal robocalling. Update as necessary.
- **Responsibility:** Legal/Compliance Lead.

Short-Term Actions (Next 2-6 months)

1. STIR/SHAKEN Implementation (Bandwidth Hosted Signing with VirtualPBX Certificate) and Testing:

- **Action:** Finalize agreement and technical setup with Bandwidth for their Hosted Signing Service, ensuring it will utilize VirtualPBX.com, Inc.'s own procured STIR/SHAKEN certificate.[2, 11, 12]

- **Action:** Develop and test the mechanism for the Kazoo platform to signal attestation levels (determined by VirtualPBX) to Bandwidth for each call. This may involve configuring custom SIP headers in Kazoo [8, 9] or API integration with Bandwidth.[12]
- **Responsibility:** Engineering Team, Technical Lead.

2. Know Your Customer (KYC) Process Enhancement:

- **Action:** Fully implement the robust KYC and customer vetting procedures detailed in Section 4.A of this report.[14, 15, 16, 17, 18]
- **Action:** Train relevant staff (e.g., sales, onboarding, support) on the new KYC protocols and risk assessment criteria.
- **Responsibility:** Operations Lead, Sales Management, Compliance Lead.

3. Basic Traffic Monitoring & Call Blocking Implementation:

- **Action:** Configure systematic analysis of Kazoo CDRs (via BigQuery) to identify suspicious calling patterns (e.g., high volume, short duration calls).[19]
- **Action:** Implement blocking of numbers on a reasonable Do-Not-Originate (DNO) list within the Kazoo callflow logic.[33]
- **Action:** Utilize Kazoo's native blocklist features and existing dialplan/network-edge blocking for known problematic numbers/IPs.[30, 31]
- **Responsibility:** Engineering Team, Operations Lead.

4. Develop Formal Traceback Response Protocol:

- **Action:** Document the internal step-by-step procedure for responding to traceback requests, ensuring the 24-hour deadline can be met. Include data extraction methods from Kazoo (CDRs via BigQuery, recordings).[1, 16, 19]
- **Responsibility:** Designated Traceback Contact, Operations Lead, Compliance Lead.

Medium-Term Actions (Next 6-12 months)

1. Advanced Robocall Mitigation Tool Implementation:

- **Action:** Evaluate, select, and implement advanced third-party analytics, reputation scoring services, and dynamic call blocking tools (e.g., solutions from YouMail [24], Ribbon [26], TransNexus [23]).
- **Action:** Integrate these tools with the Kazoo platform, potentially using Kazoo Pivot [27], APIs [28, 29], or SDKs [29] for real-time call treatment decisions.
- **Responsibility:** Engineering Team, Technical Lead, Operations Lead.

2. Ongoing Monitoring, Refinement, and Audits:

- **Action:** Establish a schedule for regular (e.g., quarterly) reviews of the robocall mitigation program's effectiveness, AUP compliance by customers, and the accuracy of the RMD filing.
- **Action:** Continuously refine mitigation tactics based on performance data, emerging threats, and any new FCC guidance.
- **Responsibility:** Compliance Lead, Operations Lead, Technical Lead.

3. Ensure Readiness for June 20, 2025, STIR/SHAKEN Deadline:

- **Action:** Ensure all necessary steps for the transition to using VirtualPBX-owned STIR/SHAKEN certificates (via Bandwidth's Hosted Signing) and self-determined attestation are completed and fully operational well in advance of the June 20, 2025, deadline.[2] This includes having the certificate deployed with Bandwidth and the attestation signaling mechanism tested and confirmed.

- **Responsibility:** Technical Lead, Compliance Lead.

Resource Allocation Considerations

- **Internal Teams:** Successful implementation will require collaboration between Engineering (for platform modifications and integrations), Technical Operations (for STIR/SHAKEN deployment, monitoring), Legal/Compliance (for RMD, AUP, policy), and potentially Customer Support (for handling customer inquiries related to call blocking or KYC).
- **Budget:** Allocate budget for potential costs, including STI-CA certificate fees, subscription fees for third-party analytics or blocking services (e.g., Google BigQuery costs), and potentially development resources if custom integration work is required for Kazoo.
- **Training:** Allocate time and resources for training staff on new KYC procedures, traceback response protocols, and the operation of any new mitigation tools.

The regulatory environment surrounding robocalls is dynamic, and the threats posed by illegal callers are constantly evolving. Therefore, VirtualPBX.com, Inc. must approach robocall mitigation not as a one-time project but as an ongoing commitment to vigilance, adaptation, and continuous improvement. The FCC has issued multiple orders and continues to refine its rules [1, 2, 3, 33], and this trend is expected to continue. Effective robocall mitigation is a cross-functional endeavor; siloed efforts are unlikely to succeed. Engineering, operations, compliance, and legal teams must work in concert to implement and maintain a robust defense against illegal robocalls.

The following table provides a consolidated action checklist:

Table 5: VirtualPBX.com, Inc. Robocall Mitigation Action Checklist

Action Item	Priority	Responsibility (Suggested Dept/Role)	Target Completion Date Range	Key Resources/Tools	Relevant Section in Report
Verify/Complete RMD Filing (DA-24-73A1)	High	Compliance Lead, Technical Lead, Legal	ASAP (within 30 days if not done)	RMD Portal, Mitigation Plan Document, Company Information	5
Initiate STIR/SHAKEN Certificate Procurement (OCN, 499-A, STI-PA, STI-CA)	High	Technical Lead, Compliance Lead	Begin within 30 days, complete steps within 3-4 months	FCC, STI-PA (iconectiv), Selected STI-CA	3, 6
Designate Traceback Point of Contact	High	Operations Lead, Compliance Lead	Within 30 days	Internal Communication, RMD Filing Update	4.D, 5, 6
Review/Update AUP & Customer Agreements	High	Legal/Compliance Lead	Within 60 days	Bandwidth AUP, Legal Counsel	4.E, 6
Finalize & Implement STIR/SHAKEN Signing Architecture (Bandwidth Hosted Signing with VirtualPBX Cert)	High	Engineering Team, Technical Lead	Design/Agreement within 60 days, Implement/Test within 4-6 months	Kazoo, Bandwidth Hosted Signing Service, VirtualPBX STIR/SHAKEN Certificate	3, 6
Develop/Test Kazoo Attestation Signaling to Bandwidth	High	Engineering Team	Concurrent with Signing Architecture (4-6 months)	Kazoo APIs/Configuration, Bandwidth API/Portal	3, 6
Implement Enhanced KYC Procedures & Training	High	Operations Lead, Sales Mgmt, Compliance	Within 3-4 months	Stripe Radar, KYC Checklist, Training Materials	4.A, 6

Implement Basic CDR Monitoring (BigQuery) & DNO/Dialplan/IP Blocking in Kazoo	Medium	Engineering Team, Operations Lead	Within 4-6 months	Kazoo CDRs, Google BigQuery, DNO Lists, Kazoo Callflows, Network Firewall	4.B, 4.C, 6
Formalize Internal Traceback Response Protocol	Medium	Designated Traceback Contact, Operations Lead	Within 3 months	Kazoo CDRs (BigQuery), Protocol Document	4.D, 6
Evaluate & Implement Advanced Mitigation Tools (Analytics, Blocking)	Medium	Engineering, Technical Lead, Operations	Evaluate within 6 months, Implement within 9-12 months	Kazoo Pivot/APIs, 3rd Party Vendor Solutions	4.B, 4.C, 6
Establish Ongoing Mitigation Review & Audit Process	Medium	Compliance Lead, Operations, Technical Lead	Within 9 months	RMD Filing, Performance Data	5, 6
Ensure Readiness for June 20, 2025 STIR/SHAKEN Deadline (using Bandwidth Hosted Signing with VirtualPBX Cert)	High	Technical Lead, Compliance Lead	Ongoing, fully operational by Q1 2025	STIR/SHAKEN Certificate, Bandwidth Hosted Signing configuration, Tested Attestation Signaling	3, 6

By diligently following this action plan, VirtualPBX.com, Inc. can significantly enhance its robocall mitigation capabilities, meet its FCC compliance obligations, and contribute to a more trustworthy telecommunications ecosystem.