

Robocall Mitigation Plan

Vyke Holding Ltd (“Vyke”) is a VoIP service provider offering mobile application-based voice services to direct retail and small business end users. Vyke does not provide SIP trunking, wholesale voice services, or bulk call origination capabilities. All voice traffic originates exclusively from authenticated end users via Vyke-controlled applications, which materially limits the potential for high-volume or automated robocall activity.

Vyke maintains a robocall mitigation program designed to prevent the origination and transmission of illegal robocall traffic, in alignment with FCC requirements.

Traceback Cooperation

Vyke complies with all traceback requests from the Federal Communications Commission (FCC), the Industry Traceback Group, law enforcement, and other authorised entities. Vyke responds promptly and in a manner consistent with industry expectations.

Vyke retains call detail records, IP address logs, timestamps, and other relevant data necessary to support traceback investigations. Vyke actively cooperates to identify the source of suspected unlawful traffic and to take immediate mitigation actions where required.

Know Your Customer (KYC)

Vyke serves only direct retail and small business end users. Vyke verifies phone numbers, email addresses, and wireless phone device integrity of all subscribers at onboarding. Payment is required for all calling services and higher volume callers are required to provide government ID and address verification. These controls establish and maintain accountability for users across the platform.

Caller ID (DID) usage is strictly controlled. Vyke validates all telephone numbers presented as Caller ID to ensure that customers are authorised to use those numbers. Vyke does not permit arbitrary or dynamic Caller ID substitution.

Vyke continuously applies additional fraud prevention controls, including monitoring of payment behaviour, account activity, and usage patterns, with thresholds and restrictions designed to identify and prevent abusive conduct. An account failing to meet these standards is suspended, pending further investigations.

Call Authentication / STIR-SHAKEN Position

Vyke does not currently implement STIR/SHAKEN authentication. In lieu of STIR/SHAKEN, Vyke relies on its robocall mitigation program and network controls to ensure the integrity of originating traffic.

All outbound calls are subject to strict Caller ID validation. Calls cannot be initiated using unverified or unauthorised numbers. Vyke issues and validates Caller IDs directly and maintains full control over number assignment within its platform.

Vyke's architecture does not support SIP interconnection, third-party traffic injection, or automated dialing systems. All calls are initiated by authenticated users via Vyke applications, with destination phone numbers manually entered or selected from user-controlled contact lists.

Vyke enforces strict call concurrency and account-level controls to prevent high-volume or automated calling patterns inconsistent with normal human usage.

Call Monitoring and Robocall Detection

Vyke operates continuous monitoring of its network using internally developed systems that generate real-time analytics, alerts, and thresholds designed to detect suspicious or non-compliant traffic.

Monitoring includes, but is not limited to:

- Call volume analysis and velocity thresholds
- Consecutive number dialing detection
- High distinct-number call rates within defined time periods
- Unusual call duration metrics and traffic patterns

Identified anomalies are subject to investigation and escalation procedures.

Enforcement and Mitigation

Vyke enforces a zero-tolerance policy for unlawful or abusive calling activity. Where suspicious or non-compliant behaviour is identified, Vyke takes immediate action, including call blocking and account termination.

Devices associated with abusive activity are permanently blocked from accessing Vyke services.

These enforcement actions are applied to prevent further origination of suspected illegal traffic and to protect downstream networks.

Network and Upstream Responsibility

Vyke maintains full control over traffic originating from its network and does not knowingly originate or transmit unlawful robocall traffic. Vyke's service model does not support third-party traffic origination or open interconnection that would increase exposure to spoofed or unauthenticated traffic.

Robocall Mitigation Program Statement

Where STIR/SHAKEN authentication is not implemented, Vyke relies on the above-described mitigation measures, including customer verification, Caller ID validation, traffic monitoring, and enforcement controls, to prevent the origination and transmission of illegal robocall traffic in accordance with FCC rules.

Material Change Commitment

Vyke certifies that the information contained in this filing is accurate and complete to the best of its knowledge.

Vyke commits to updating its Robocall Mitigation Database filing within 10 business days of any material change to its robocall mitigation program, STIR/SHAKEN implementation status, or business operations that may affect compliance.

Vyke maintains internal governance and compliance processes to identify, assess, and promptly reflect such changes in its filing.