

Know Your Customer (KYC) Plan – Natural GC

As part of our Robocall Mitigation Program, Natural GC implements a structured Know Your Customer (KYC) process designed to identify, assess, and mitigate potential sources of illegal robocall traffic. Our procedures apply to both new and existing customers, ensuring ongoing compliance and network integrity.

1. Customer Identification and Verification

We collect and verify the following information before activating any voice services:

- Full legal name / business name
- Business registration documents
- Tax ID (EIN) or national ID for individuals
- Contact information (email, phone, address)
- Description of business use case for telecom services
- Authorization proof for outbound voice traffic, if applicable

2. Third-Party Analytics

At this time, Natural GC does not use a third-party vendor for call analytics. However, we perform in-house monitoring and analysis of traffic patterns using our network's logging and alerting tools. We are evaluating third-party solutions to enhance detection and mitigation efforts.

3. Traffic Monitoring & Pattern Analysis

Our internal systems monitor call behavior in real-time, flagging abnormal traffic such as:

- Excessive short-duration calls
- High call volume to known DNO (Do Not Originate) numbers
- Repeated calls with high failure or rejection rates

Suspicious traffic is immediately investigated, and if necessary, service is suspended pending further review.

4. Ongoing Review of Existing Customers

Natural GC performs periodic audits of active customer traffic to ensure compliance with our Acceptable Use Policy. Customers with anomalies are contacted to provide clarification, and services may be adjusted or terminated as needed.

5. Mitigation and Enforcement Steps

If illegal robocall traffic is detected:

- Immediate suspension of service
- Internal investigation of call records and usage
- Customer notification and request for explanation
- Escalation to legal team if warranted
- Reporting to appropriate regulatory authorities when necessary

6. Customer Education

We provide all customers with guidelines regarding prohibited robocall activity, TCPA compliance, and our mitigation policy at the time of onboarding.

Preventing Illegal and Fraudulent Calls with Fail2Ban in SIPWISE.

Within our SIPWISE softswitch platform, we have implemented Fail2Ban as an additional security layer to protect our VoIP infrastructure against unauthorized access, fraud, and illegal calling attempts.

Fail2Ban continuously monitors system logs and SIP traffic for suspicious patterns, such as repeated failed authentication attempts, unusual calling behavior, or SIP scanning activities. When such patterns are detected, it automatically blocks the offending IP address using firewall rules, preventing the attacker from continuing any malicious activity.

This mechanism is particularly effective in mitigating:

- Brute-force attacks on SIP accounts
- Mass extension scanning attempts
- Unauthorized international call attempts
- Peering fraud or misuse of system resources

Through its integration with SIPWISE, Fail2Ban responds in real time and autonomously, significantly reducing the risk of financial losses due to fraud and improving overall service integrity. Additionally, our team can monitor these events and adjust security policies as needed. In summary, Fail2Ban strengthens the security of our SIPWISE environment by ensuring that only legitimate users can access and use the system, while actively blocking potential threats.