



Robocall Mitigation – Infinexy Technologies LLC (FRN: 0038780078)

Infinexy Technologies LLC is a privately owned company. The company acts as an intermediate voice services provider that doesn't have its own subscriber base within the United States.

As a voice service provider, Infinexy is in the process of implementation anti fraud call authentication framework into our network infrastructure and will integrate it as soon as possible.

Robocall Mitigation Program

Infinexy Technologies LLC maintains a robocall mitigation program designed to take reasonable steps to reduce the origination, carrying, and/or processing of illegal robocall traffic through its network.

The program combines STIR/SHAKEN authentication where technically supported with customer due diligence, traffic monitoring, analytics, traceback cooperation, abuse investigation, and other controls appropriate to Infinexy's network and services.

Customer and Traffic Due Diligence

Infinexy Technologies LLC will apply appropriate controls to identify and assess customers and traffic sources, including, as applicable:

Verification of customer identity and business information before service activation;

Review of customer use cases and expected calling patterns;

Collection and review of applicable customer contact and authorization information;

Review of numbering resources and caller-ID practices;

Risk-based review of customers generating unusually high-volume or anomalous traffic;

Additional scrutiny of customers or traffic exhibiting characteristics associated with illegal robocalling or spoofing; and

Suspension, restriction, or termination of traffic or accounts when warranted by applicable contractual, regulatory, or network-abuse requirements.



STIR/SHAKEN Controls

For IP-based traffic within the portions of its network where STIR/SHAKEN has been implemented, Infinexy Technologies LLC will:

Authenticate eligible originating calls in accordance with applicable STIR/SHAKEN requirements;

Apply the appropriate attestation level based on the provider's relationship with the originating customer and calling number;

Protect authentication credentials and certificate-related infrastructure;

Preserve and transmit authenticated caller-ID information as required when handling authenticated traffic; and Monitor implementation coverage and expand STIR/SHAKEN deployment as applicable.

For traffic or network segments not currently capable of STIR/SHAKEN authentication, Infinexy Technologies LLC will use the alternative mitigation measures described in this plan.

Caller-ID and Spoofing Controls

Infinexy Technologies LLC monitors for suspicious caller-ID activity, including patterns that may indicate:

Unreasonable or anomalous use of telephone numbers;

Invalid, unavailable, or inconsistent caller-ID information;

High-volume calling inconsistent with the customer's stated use case;

Rapid changes in calling-number behaviour;

Suspected spoofing; or

Other indicators of potentially unlawful or abusive traffic.

Where appropriate, suspicious traffic may be investigated, restricted, suspended, or referred for additional review.

Ongoing Program Review

Infinexy Technologies LLC will periodically review its robocall mitigation controls and update its procedures as appropriate based on:

Changes in FCC requirements;

Changes in STIR/SHAKEN deployment;

Emerging robocall and spoofing techniques;
Customer and traffic-risk trends;
Traceback findings;
Industry best practices; and
Internal monitoring and incident experience.

Traffic Analytics and Monitoring

Infinexy Technologies LLC uses reasonable technical and operational measures to identify potentially abusive traffic. Depending on the service and network segment, these measures may include:

Call-volume monitoring;
Call-pattern and velocity analysis;
Destination analysis;
Caller-ID anomaly detection;
Customer-level traffic profiling;
Reputation and risk indicators;
Manual review of suspicious activity; and
Escalation of suspected illegal robocall activity to appropriate personnel.

Specific thresholds and detection methodologies may be adjusted as threat patterns and network conditions evolve.

Investigation and Enforcement

When Infinexy Technologies LLC identifies or receives credible information concerning suspected illegal robocalling, spoofing, or related abuse, it may:

Investigate the relevant customer, traffic, and call records;
Identify the source and scope of the activity;



Request additional information from the customer or upstream/downstream provider;
Restrict or suspend suspicious traffic where appropriate;
Terminate service for confirmed or persistent violations when warranted;
Preserve relevant records; and
Cooperate with regulatory, law-enforcement, and traceback inquiries.

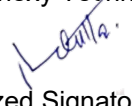
Implementation Limitations and Mitigation

Because Infinexy Technologies LLC currently has partial rather than full STIR/SHAKEN implementation, the company recognizes that not all IP-based traffic may presently receive STIR/SHAKEN authentication.

For those portions of the network, Infinexy Technologies LLC relies on the alternative controls described above, including customer verification, traffic monitoring, anomaly detection, investigation, traceback cooperation, and appropriate traffic/account enforcement.

The company will continue evaluating technical and operational opportunities to increase STIR/SHAKEN coverage.

For, Infinexy Technologies Limited


Authorized Signatory