



Robocall Mitigation Plan – Carden IT Services, LLC

Company Name: Carden IT Services, LLC

FCC Registration Number (FRN): 0031699846

Primary Contact/Compliance Officer:

- Name: Jeremy Huson
- Title: Compliance Officer
- Phone: 917-671-7691
- Email: jeremy.huson@cardenitservices.com

Address: 85 Broad St, FL18, New York, NY, 10004

1. STIR/SHAKEN Implementation Status

Current Status: Fully implemented STIR/SHAKEN Imdeployment

Carden IT Services, LLC (“Carden IT”) provides SIP-based business voice services to enterprise customers using a hosted 3CX platform. Carden IT has fully implemented the STIR/SHAKEN caller ID authentication framework on the IP portions of its network used to originate calls to the public switched telephone network (PSTN).

Carden IT delivers outbound NANP traffic to its underlying carrier, Telonium, which authenticates and signs Carden IT’s traffic using an STI certificate issued in accordance with industry standards and FCC rules. As a result, all eligible IP-originated outbound calls to the PSTN are authenticated with STIR/SHAKEN before they are handed off for termination.

Carden IT periodically reviews signing performance and attestation levels available from Telonium, including call analytics and any alerts related to call authentication or potential abuse, to ensure continued alignment with FCC requirements and industry best practices. Where appropriate, Carden IT may adjust routing, customer profiles, or service configurations to maintain the integrity of authenticated traffic.



2. Customer Vetting and Onboarding (KYC)

Carden IT Services LLC provides services only to verified, direct business end-users located in the United States. No resellers, downstream carriers, traffic aggregators, marketing lead dialers, or bulk originators are permitted.

All customers undergo comprehensive KYC screening prior to activation, including:

- Verification of legal business entity via state registration and EIN
- Physical U.S. business address (no PO boxes)
- Identification of responsible officer with direct contact information
- Call purpose and traffic usage review (type, geography, expected volume)
- Validation of number authorization for all caller ID values used
- Direct operational relationship with configuration oversight of customer phone systems
- Mandatory security controls to prevent unauthorized dialer injection or exploit pathways
- Either in person meeting or video call to verify the user.

Customers failing identity verification, numbering rights validation, or lawful use screening are not activated.

3. Robocall Monitoring and Analytics

Carden IT maintains ongoing monitoring and analytics across all originated voice traffic, including fully authenticated calls, to detect patterns that may indicate illegal or abusive robocalling. This monitoring includes, but is not limited to:

- Call volume and call-per-second (CPS) thresholds by customer and trunk group;
- High-risk call patterns (e.g., very short-duration calls, unusual answer/seizure ratios, or high-volume bursts to specific destinations);
- Call attempts to known invalid, unallocated, or high-risk number ranges; and



- Complaints or feedback from downstream carriers, Telonium, end users, or regulators.

When internal monitoring, Telonium, or downstream carriers identify suspicious traffic, Carden IT performs a structured review of the affected customer, traffic profile, and use case. Depending on the outcome of that review, Carden IT may issue warnings, apply additional rate limits or restrictions, require updated KYC or use-case documentation, or suspend/terminate service as described in this plan.

4. Enforcement and Remediation Procedures

If suspicious or unlawful calling behavior is detected:

1. Immediate suspension of outbound call privileges
2. Customer notification and remediation request
3. Verification and audit review prior to reinstatement
4. Permanent termination if remediation fails or abuse is confirmed

All enforcement actions are documented and retained for regulatory review.

5. Call Authentication and Blocking

Carden IT's call authentication and blocking practices are designed to prevent the origination of illegal robocalls and unlawful spoofing while preserving legitimate traffic for business customers.

All eligible outbound calls originated by Carden IT customers are authenticated using STIR/SHAKEN by Telonium, which signs Carden IT's traffic using an STI certificate in accordance with FCC rules and industry standards. Carden IT configures its platform to ensure that customer-presented caller IDs are consistent with the customer's authorized numbers and with Telonium's signing policies.

Carden IT prohibits customers from using caller ID numbers for which they do not have a legitimate right of use and enforces this through configuration controls and its Acceptable Use Policy. Where unauthorized or suspicious caller ID usage is detected, Carden IT may block such calls, require documentation of number ownership, or modify configurations to restrict caller ID options.



Carden IT also cooperates with reasonable blocking and labeling practices implemented by Telonium and downstream carriers, and will work with affected customers to remediate any mislabeling concerns where traffic is determined to be lawful and compliant.

6. Compliance Oversight

- **Compliance Officer:** Jeremy Huson
- Responsible for mitigation enforcement, traceback response, customer vetting, and suspension authority
- All traceback requests are acknowledged and responded to within **24 hours**
- Policy review occurs annually or upon FCC rule changes

Carden IT has designated a Robocall Compliance Officer who is responsible for overseeing this Robocall Mitigation Plan, coordinating with Telonium and other underlying providers on STIR/SHAKEN implementation and related controls, reviewing monitoring and enforcement.

7. Prior Administrative Status

Carden IT Services LLC acknowledges past Robocall Mitigation Database administrative removal related to documentation misalignment and attestation categorization. No findings of unlawful robocalling, spoofing behavior, or consumer harm were made, and no financial penalties were issued.

This revised filing, combined with updated certification status and STIR/SHAKEN implementation commitment, resolves all prior administrative deficiencies.

8. Certification

Carden IT Services LLC certifies that:

- Full mitigation, KYC enforcement, and analytics monitoring are applied to all originated traffic during the temporary unsigned period.
- Full STIR/SHAKEN signing will commence immediately upon SPC token issuance and STI certificate activation.



- Carden IT Services LLC will update its RMD certification to **Full Implementation** within ten (10) business days post-activation.
- The Company acknowledges the **September 18, 2025** STIR/SHAKEN compliance deadline and certifies its alignment with the federal implementation requirement.

Signed:

A handwritten signature in black ink that reads 'J. Huson'.

Jeremy Huson

Compliance Officer

12/11/2025