

ROBOCALL MITIGATION PLAN

inContact, Inc.

Updated: 7/1/2026

I. Provider Identification

Provider Name: inContact, Inc.

Primary Address:

75 W. Towne Ridge Parkway, Tower 1
Sandy, UT 84070

FCC Registration Number: 0004977997

Operating Company Number(s): 186B, 322F

Other Business Name(s): NICE, NICE CXone, NICE inContact

Previous Business Name(s): Buyers United, Inc.; UCN, Inc.

Merged or Consolidated Entities with Prior Separate RMD Filings: VoApps, Inc.; LiveVox, Inc.; Engage Holdings LLC; BusinessPhone

Contact for Robocall Mitigation-Related Issues:

Robert Vukich

Director, Product Management

Telecom

75 W. Towne Ridge Parkway, Tower 1
Sandy, UT 84070

Telephone: 801-531-4092

Email: Robert.vukich@nice.com

Traceback Contact:

Kristi Thornley

Compliance Specialist / Senior Paralegal - Contracts & Compliance Specialist
Legal

75 W. Towne Ridge Parkway, Tower 1
Sandy, UT 84070

Telephone: 801-715-5154

Email: compliance@niceincontact.com; Kristi.thornley@nice.com

II. Provider Role in the Call Chain

inContact, Inc. is a Voice Service Provider with a STIR/SHAKEN implementation obligation serving end users.

inContact provides cloud-based contact center and related communications services to business customers. inContact uses Voice over Internet Protocol technology as the primary

method to connect inContact customers to their customers, end users, and other call recipients. inContact is not generally available to the public as an open-access voice service provider. Access to the inContact voice network is limited to business customers that have contracted with inContact and are subject to contractual, technical, operational, and compliance controls.

inContact does not accept or process traffic for unaffiliated upstream voice service providers. inContact processes traffic from its contracted business customers, allowing inContact to identify the customer source of traffic on its network and to investigate and address suspected unlawful or abusive traffic.

III. Merged or Consolidated Entities with Prior RMD Filings

Effective January 1, 2026, certain affiliated entities that previously maintained separate Robocall Mitigation Database filings were merged into, integrated with, or otherwise consolidated under inContact, Inc. These entities include VoApps, Inc.; LiveVox, Inc.; Engage Holdings LLC; and BusinessPhone.

As a result of these mergers or consolidations, those entities no longer maintain separate active RMD filings. Any prior FRNs, OCNs, or RMD identifiers associated with those entities are retired or no longer used for current operations and are not listed as current inContact identifiers.

Any active voice operations, traffic, customers, numbers, services, or related robocall mitigation obligations formerly associated with those entities and now operated by inContact are subject to inContact's robocall mitigation program described in this Plan.

IV. STIR/SHAKEN Implementation

inContact is not relying on any exemption or extension pursuant to 47 C.F.R. § 64.6304(d). inContact has fully implemented STIR/SHAKEN in the IP portions of its network.

inContact uses the following third-party vendors and/or underlying carriers to sign calls:

- Affinity Network, Inc.
- Peerless
- AT&T
- Sinch
- Bandwidth
- Teliax
- CenturyLink d/b/a Lumen
- Verizon
- IMPACT

inContact's STIR/SHAKEN implementation is designed to authenticate caller ID information for applicable SIP/IP-originated U.S. domestic outbound calls. inContact applies attestation

practices based on the level of confidence in the customer's authorization to use the calling number.

Where numbers are obtained from or managed by inContact, inContact has direct visibility into number assignment and authorization. Where customers use telephone numbers not obtained from inContact, inContact requires appropriate evidence of authorization, which may include a letter of authorization, authorized signature, carrier records, account documentation, or other evidence reasonably sufficient to validate the customer's right to use the number.

For a customer to receive A-level authentication, the customer must either purchase or obtain the relevant DIDs or toll-free numbers from NICE/inContact, or provide documentation validating the customer's right to use the number. Numbers for which inContact has a lower level of confidence may receive lower attestation treatment, and unauthorized numbers may be restricted or blocked.

V. Robocall Mitigation Program

All calls that originate on inContact's network are subject to a robocall mitigation program designed to identify the source of traffic and prevent that source from continuing to originate traffic of the same or similar unlawful, suspicious, or abusive nature.

inContact's mitigation program includes the following reasonable steps:

1. customer due diligence and know-your-customer controls;
2. contractual prohibitions on unlawful, fraudulent, abusive, or unauthorized use of inContact services;
3. number authorization and caller ID controls;
4. STIR/SHAKEN authentication for applicable IP-originated calls;
5. call analytics, monitoring, and proprietary review tools;
6. complaint, abuse, and traceback response procedures;
7. processes to restrict, block, suspend, or terminate unlawful or abusive traffic;
8. public safety safeguards;
9. procedures addressing providers listed or not listed in the Robocall Mitigation Database; and
10. ongoing review and update of the RMD filing and mitigation plan.

inContact does not knowingly permit its services to be used to originate, carry, process, or transmit illegal robocalls, unlawful spoofing traffic, fraudulent traffic, or other illegal voice traffic. If inContact identifies unlawful, unauthorized, suspicious, or abusive use of its platform or network, inContact may take corrective action, including customer notice, investigation, traffic blocking, number-use restriction, suspension of calling capabilities, termination of service, or referral to law enforcement or regulators.

VI. Know-Your-Customer Procedures

inContact provides services to contracted business customers and does not sell or provide access to anonymous third parties. Customers must contract with inContact for software, voice, or related services before they are permitted to use the inContact network.

inContact's know-your-customer procedures include, as applicable:

1. identifying the customer's business entity and authorized account representatives;
2. collecting customer contact, billing, and account-administration information;
3. conducting credit checks and associated background review;
4. requiring customers to accept contractual terms governing use of inContact services;
5. requiring customers to comply with applicable law, including laws governing robocalls, caller ID, consent, telemarketing, Do Not Call, and spoofing;
6. limiting platform access to authenticated and authorized customer users;
7. validating customer authority to use telephone numbers and caller ID information;
8. monitoring customer-specific complaints, traceback requests, carrier notices, and abuse indicators; and
9. escalating suspected illegal, fraudulent, or abusive conduct to appropriate internal teams.

Because inContact's services are provided to identifiable business customers, inContact can identify the customer source of traffic on its network, including the relevant customer account and, where available, more granular call-originating information. This allows inContact to investigate suspected unlawful or abusive traffic and to require corrective action from the responsible customer.

VII. Contractual Controls

inContact's customer agreements and terms of use prohibit illegal, fraudulent, abusive, misleading, or unauthorized use of inContact software, platform, and network services. Customers are required to comply with all applicable laws and regulations in their use of inContact services.

inContact's standard terms and conditions permit corrective action, up to and including suspension or termination of service, if fraudulent, illegal, or abusive traffic is identified. Customers must also comply with applicable network connectivity terms before they are permitted to use the inContact network.

When inContact receives inquiries, traceback requests, complaints, carrier notices, or other indicators of potential customer misconduct, inContact may contact the customer, advise the customer of the issue, require an explanation or remediation, and notify the customer that continued misconduct may violate the customer's agreement and terms of use. Where appropriate, inContact may restrict traffic, suspend calling privileges, block numbers or traffic, or terminate the customer's service.

VIII. Number Authorization and Caller ID Controls

inContact uses number authorization controls to reduce the risk of unlawful spoofing and unauthorized caller ID use. Customers may use telephone numbers acquired through inContact/NICE or, where supported and approved, customer-provided numbers.

For numbers acquired through inContact/NICE, inContact has direct visibility into the number assignment relationship and can use that information to support STIR/SHAKEN attestation decisions. For customer-provided numbers, inContact may require evidence that the customer owns, controls, or is otherwise authorized to use the number.

If inContact determines that a customer lacks authorization to use a number, inContact may reject or restrict use of the number, require additional documentation, modify the attestation level, block traffic, suspend outbound calling capabilities, or terminate service.

IX. Call Analytics Systems Used to Identify and Block Illegal Traffic

inContact uses tools including Ribbon Analytics, Empirix, and proprietary tools to monitor and manage calls. These tools support inContact's ability to identify potentially suspicious, abusive, unlawful, or noncompliant calling patterns and to investigate the source of traffic.

As part of its STIR/SHAKEN implementation, inContact has identified numbers acquired from inContact/NICE to support accurate identification of number ownership and appropriate attestation decisions. inContact's number validation and attestation processes help determine whether A-level or B-level attestation is appropriate for a given call.

inContact does not originate gateway traffic and does not accept traffic from unaffiliated upstream providers for processing. Accordingly, inContact does not expect its traffic to qualify for C-level attestation based on unknown or unauthenticated upstream origination.

inContact's software also provides legally compliant time-of-day and Do Not Call tools for customers. These tools help customers manage outbound calling practices and reduce the risk of calling during prohibited times or contacting individuals who should not be called.

Where inContact identifies traffic that appears unlawful, fraudulent, unauthorized, suspicious, spoofed, or otherwise abusive, inContact may take one or more of the following actions:

1. block or restrict traffic;
2. restrict use of specific telephone numbers or caller ID information;
3. require customer explanation, documentation, or remediation;
4. suspend outbound calling for the affected account, campaign, user, or customer;
5. modify STIR/SHAKEN attestation treatment where appropriate;
6. terminate customer access to voice services;
7. coordinate with downstream carriers, analytics providers, or traceback participants;

8. respond to regulatory, law enforcement, or traceback requests; and
9. preserve relevant records as appropriate.

X. Know-Your-Upstream-Provider Procedures

inContact does not accept or process traffic for other upstream providers. inContact processes traffic from its own contracted business customers. Because inContact does not accept unaffiliated upstream-provider traffic, inContact can trace traffic to the responsible customer source and can address illegal or suspicious traffic through its customer controls, contractual remedies, number authorization procedures, analytics tools, traceback response, and abuse-response processes.

To the extent inContact works with underlying carriers, downstream providers, transit providers, terminating providers, or other service providers for call signing, routing, completion, traceback, or mitigation purposes, inContact coordinates with those providers regarding suspicious traffic, traceback requests, attestation issues, number authorization, RMD status, blocking, labeling, and other robocall mitigation matters as appropriate.

inContact complies with applicable prohibitions on accepting traffic from providers that are not listed in the Robocall Mitigation Database or whose certifications have been removed by Commission action.

XI. Traceback Requests and Cooperation

inContact is committed to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the registered industry traceback consortium, and to cooperating with such entities in investigating and stopping illegal robocallers that use inContact's service to originate, carry, or process calls.

inContact maintains internal procedures for receiving, triaging, investigating, and responding to traceback requests. These procedures may include identifying the customer, account, telephone number, call path, timestamp, originating station or agent information, authentication information, routing information, and other relevant details; coordinating with internal network, compliance, legal, security, and customer-support teams; requesting information from customers or providers where needed; preserving relevant records as appropriate; and taking corrective action where the investigation identifies unlawful or abusive use.

XII. Industry Traceback Group and Do-Not-Originate Requests

inContact follows Industry Traceback Group recommended practices, as applicable. inContact has mechanisms in place to promptly respond to Do Not Originate requests received from the Industry Traceback Group.

Notifications are routed to inContact's compliance contact and escalated to the appropriate network management or operations team. Where appropriate, inContact can

add relevant numbers or addresses to internal databases, block or restrict traffic, and notify the responsible customer or party to cease the prohibited conduct.

XIII. Public Safety Safeguards

inContact makes reasonable efforts to ensure that it does not block calls from public safety answering points, emergency services, or government emergency numbers. inContact maintains 911 service capabilities and uses special routing designed to prioritize 911 calls to the appropriate local public safety answering point.

Robocall mitigation, analytics, blocking, and traffic restriction measures are implemented with the objective of reducing illegal traffic while avoiding inappropriate blocking of emergency calls, public safety communications, and other protected communications.

XIV. Prior Regulatory, Law Enforcement, or Commission Actions

To the best of inContact's knowledge after reasonable inquiry, during the prior two years, neither inContact nor any entity for which inContact shares common ownership, management, directors, or control has been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or due to a deficient Robocall Mitigation Database certification or robocall mitigation program description.

If this statement is not accurate, inContact will provide a description of each action or investigation, including the agencies involved, the date commenced, current status, summary of findings, and whether any final determinations have been issued.

XV. RMD and CORES Information Maintenance

inContact will maintain its Robocall Mitigation Database filing and related CORES information so that the information remains accurate and current. inContact will update its RMD filing within 10 business days of any change to information required by applicable FCC rules, including changes to provider information, business names, prior business names, responsible robocall mitigation contact, traceback contact, STIR/SHAKEN implementation status, role in the call chain, OCN, robocall mitigation program, analytics systems or vendors, traceback commitment, or required regulatory/enforcement disclosures.

inContact will complete applicable annual RMD recertifications by the FCC's annual deadline and will confirm that the information submitted to the RMD is true and correct at the time of recertification.

XVI. Certification Support Statement

inContact has implemented a robocall mitigation program that includes reasonable steps to avoid originating, carrying, processing, or transmitting illegal robocall traffic and unlawful spoofing traffic. inContact's mitigation program includes customer due diligence,

contractual use restrictions, number authorization controls, STIR/SHAKEN authentication for applicable IP-originated traffic, call analytics and monitoring, complaint and abuse response, traceback cooperation, provider coordination, public safety safeguards, and corrective action.

inContact is committed to cooperating with the FCC, law enforcement, the registered industry traceback consortium, and appropriate industry participants to investigate and stop illegal robocallers that attempt to use inContact's services.