



February 23, 2026

ConvergeOne, Inc. ("C1")

Robocall Mitigation

Filing Date: February 23, 2026

FCC Registration Numbers ("FRNs"): 0011951522 & 0036282606

Specific Reasonable Steps Taken to Avoid Originating Illegal Robocall Traffic

All calls that originate on C1's network are subject to a robocall mitigation program ("RMP"), which includes (a) reasonable steps to avoid originating illegal robocall traffic, (b) a commitment to respond fully and in a timely manner to all traceback requests from the Federal Communications Commission ("FCC"), law enforcement, and the registered consortium, and (c) to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

A robocall is an unsolicited call from an auto-dialer that delivers a prerecorded voice message, and the specific reasonable steps C1 has taken to avoid originating illegal robocall traffic varies depending on the type of offering purchased by the customer. C1 resells telephony services that are solely provided by third parties ("Resold Telephony Services"). C1 also provides Internet Protocol ("IP") Enabled Services that include Branded Calling Identification ("BCID") features and a complete STIR/SHAKEN implementation ("IP Enabled Services"). The robocall mitigation measures applicable to C1's Resold Telephony Services and IP Enabled Services offerings are separately described below.

C1 has not been prohibited from filing a certification in the Robocall Mitigation Database, and C1 does not have a history of enforcement actions for illegal robocalls, Telephone Consumer Protection Act ("TCPA") or the Telemarketing Sales Rule ("TSR") violations, or related state law violations.

A. RESOLD TELEPHONY SERVICES

At this time, C1 has not implemented the STIR/SHAKEN authentication framework on any portion of its network when it provides Resold Telephony Services.

1. STIR/SHAKEN

- a. C1 at this time has not implemented the STIR/SHAKEN authentication framework on any portion of its network that provides Resold Telephony Services. When it provides Resold Telephony Services, C1 is a reseller, as defined by the FCC (*See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3260, ¶ 40 (2020) (excluding from a STIR/SHAKEN implementation obligation those providers that lack control over the necessary network infrastructure); *Call Authentication Trust Anchor*, Second Report and Order, 36 FCC Rcd 1859, 1868, ¶ 19 (2020)) that lacks control of the network infrastructure necessary to implement the framework.



2. Know Your Customers

- a. C1 performs a formal know your customers (“KYC”) vetting process on new and renewing customers of Resold Telephony Services based on guidelines set forth by the Cellular Telephony Industry Association (“CTIA”) for their BCID initiative. This vetting process will include, but not be limited to, collecting data such as Legal Name and Domestic Jurisdiction of Incorporation/Registration, Assumed/Fictitious Names (“DBAs”) utilized by the Organization, Organization Website, Organization Type and Physical Address, Dun & Bradstreet Number (“DUNS”) Report, Billing Contact and Address, Authorizer Name and Email, Primary Business Domain (SIC Code), Corporate Registration Number, etc.
- b. Furthermore, C1 has provisions in its customer agreements for new and renewing customers requiring customers to represent and warrant that all use of C1’s services will at all times comply with all applicable law, including but not limited to the rules, policies, and regulations of the FCC. Failure to comply with such obligations would be a material breach of the agreement, which would allow C1 to suspend services, terminate the agreement immediately, or take any other action C1 deems necessary to enforce the terms of the agreement.

3. Call Blocking and Filtering

- a. C1 utilizes a small number of providers to provide Resold Telephony Services.
- b. C1 confirms that each such provider has a certification in the Robocall Mitigation Database (“RMD”). We will not accept voice traffic, or obtain telephony services for resale, from an unregistered provider.
- c. C1’s agreements with such providers require that the provider comply with all applicable laws. When it provides Resold Telephony Services, C1 does not use analytics provided by any third party for purposes of call blocking or filtering.

4. Traceback

- a. C1 commits to respond fully to all traceback requests from the FCC, law enforcement, and the registered consortium within twenty-four (24) business hours of C1’s receipt of such request, as more specifically defined in 47 CFR § 64.1200(n)(1). C1 cooperates fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

5. Monitoring

- a. C1 utilizes a small number of providers to provide Resold Telephony Services.
- b. C1 confirms that each such provider has a certification in the RMD. We will not accept voice traffic, or obtain telephony services for resale, from an unregistered provider.



- c. C1's agreements with such providers require that the provider comply with all applicable laws.
- d. When it provides Resold Telephony Services, C1 does not use analytics provided by any third party for purposes of network monitoring.

6. Upstream Providers.

- a. C1 utilizes a small number of providers to provide Resold Telephony Services.
- b. C1 confirms that each such provider has a certification in the RMD. We will not accept voice traffic, or obtain telephony services for resale, from an unregistered provider.
- c. C1's agreements with such providers require that the provider comply with all applicable laws.

B. IP-ENABLED SERVICES

C1 also provides certain customers with IP Enabled Services, which include BCID features. When C1 provides IP Enabled Services, C1 is a service provider with a STIR/SHAKEN implementation obligation serving end-users.

C1 uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls in connection with the provision of IP Enabled Services:

1. STIR/SHAKEN

- a. C1 has registered with the STIR/SHAKEN Policy Administrator ("STI-PA") using OCN 071L. We have our own STIR/SHAKEN certificate issued by the BCID Certification Authority ("STI-CA") that we use when authenticating all calls that we originate through our IP Enabled Services. We have implemented a STIR/SHAKEN solution supplied by TransNexus.

2. Know Its Customers

- a. C1 performs a formal KYC vetting process on new and renewing customers based on guidelines set forth by the CTIA for their BCID initiative. This vetting process will include but not be limited to collecting data such as Legal Name and Domestic Jurisdiction of Incorporation/Registration, DBAs utilized by the Organization, Organization Website, Organization Type and Physical Address, DUNS Report, Billing Contact and Address, Authorizer Name and Email, Primary Business Domain (SIC Code), Corporate Registration Number, etc.
- b. Our contractual provisions with new and renewing customers prohibit them from initiating illegal robocalls. C1 has provisions in its customer agreements requiring customers to represent and warrant that all use of C1's services will at all times comply with all applicable law, including but not limited to the rules, policies, and regulations of



the FCC. Failure to comply with such obligations would be a material breach of the agreement, which would allow C1 to suspend services, terminate the agreement immediately, or take any other action C1 deems necessary to enforce the terms of the agreement. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we terminate their service.

3. Traceback

- a. C1 commits to respond fully to all traceback requests from the FCC, law enforcement, and the registered consortium within twenty-four (24) business hours of C1's receipt of such request, as more specifically defined in 47 CFR § 64.1200(n)(1). C1 cooperates fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

4. Robocall Mitigation Program

- a. When providing IP Enabled Services, C1 uses call analytics software provided by TransNexus to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls.
- b. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if we process outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.
- c. C1 performs the same mitigation steps for all outbound calls, regardless of our role in the call chain for a particular call.
- d. We promptly investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

5. Upstream Providers.

- a. We have a vetting and review process for upstream providers, that is, providers that send us voice traffic that we terminate or transit to other providers.
- b. We confirm that the upstream provider has a certification in the Robocall Mitigation Database. We will not accept voice traffic from a provider that does not have a current certification in the Robocall Mitigation Database.
- c. We require that upstream providers have a reasonable robocall mitigation plan, including a vetting process for their customers and upstream providers, and use call analytics to identify suspicious traffic.



- d. C1 continues to review and amend its vendor agreements, as needed, to reflect each carrier's obligation to mitigate the origination and processing of illegal robocalls.
- e. We establish an understanding of the upstream provider's role in the call path for the traffic they will send to us, for example, whether they are acting as an originating voice service provider, a foreign intermediate provider, or a U.S.-based intermediate provider.

C. OWNERSHIP AND AFFILIATES

- 1. C1 is a wholly-owned subsidiary of ConvergeOne Holdings, Inc.
- 2. Currently, all of C1's wholly-owned subsidiaries and affiliates are as follows: AAA Network Solutions, Inc.; ConvergeOne Dedicated Services, LLC; ConvergeOne Government Solutions, LLC; ConvergeOne India Private Limited; ConvergeOne Managed Services, LLC; ConvergeOne Systems Integration, Inc.; ConvergeOne Technology Utilities, Inc.; OneTech Solutions, LLC; ConvergeOne Unified Technology Solutions, Inc.; Integration Partners Corporation; NetSource Communications, Inc.; NuAge Experts, LLC; and SPS - Providea Limited.
- 3. C1's director is currently: Jeffrey Russell.
- 4. C1's officers are currently: Jeffrey Russell (Chief Executive Officer & President), David Croxville (Chief Financial Officer & Treasurer), and Rui Goncalves (General Counsel & Secretary).