**Credo Technology Group, LLC**

# Robocall Mitigation Program Description

October 30, 2026 | 47 CFR Section 64.6305(d)(2)(ii)-(iii)

Credo Technology Group, LLC (CTG) provides hosted VoIP service as a reseller of CoreDial, LLC (the wholesale provider). CTG manages customer phones and settings within the wholesale provider's platform. This program applies to CTG's voice service customers and combines CTG's customer verification, usage review, and abuse response with the wholesale provider's network-level mitigation program.

## 1. New customer verification

CTG personally meets its customers before accepting them for service. Customers are typically existing IT or web services clients. CTG verifies a business customer's valid business license or a residential customer's local residence and checks that information against the customer's other documentation. CTG does not accept customers it has not met and does not allow self-service account signup.

## 2. Continuing customers and renewals

CTG maintains regular contact with its clients through its ongoing service relationships and knows their identities, locations, and business activities. For continuing or renewing customers, that contact supports ongoing verification. If CTG has not been in contact with a client for a while, it revalidates the client using its customer-verification process.

## 3. Usage review, call analytics, and network blocking

CTG customers have metered calling rather than unlimited calling plans. Unexpectedly large bills provide a warning sign of increased outbound calling and a reason to review the account. CTG's own review is manual; it does not operate a separate automated call analytics system.

For network-level analytics and call blocking, CTG relies on the wholesale provider's program. The provider's publicly filed mitigation plan describes traffic monitoring using YouMail Watch Call Detail Record service (YouMail CDR), a commercial Do Not Originate (DNO) list from Somos, an internal DNO list, and internal analytics that examine irregular or unexpected calling patterns and calling-number use against customer profiles. The filed plan also describes anti-spoofing tools to identify and block illegal calls. These are provider-reported network controls, operated by the wholesale provider.

## 4. Wholesale provider verification and coordination

In preparing this program, CTG reviewed its wholesale provider's public FCC Robocall Mitigation Database entry, RMD0002771, and its filed mitigation plan on October 30, 2026. The entry was published in the database. The review covered the provider's identity and wholesale role, customer-verification measures, traffic analytics, blocking practices, and contractual restrictions against misuse.

CTG maintains a direct reseller relationship with the wholesale provider and works with it to investigate reported misuse, report account-security actions, request follow-up monitoring, and address continued abuse through extension-level or account-level suspension.

### 5. Contractual safeguards

CTG's updated Service Activation Form includes a lawful-use, account-security, and abuse-response provision expressly included in the customer's signature acknowledgment. It prohibits illegal robocalls, fraud, unlawful caller-ID spoofing, and other unlawful traffic. Customers must safeguard credentials and telephone equipment, report suspected unauthorized access or misuse, and cooperate with investigation and corrective action. The added provision applies to each customer upon that customer's acceptance of the updated form.

Subject to applicable law, the form permits immediate restriction or suspension when specific reports, call records, or other information reasonably indicate unlawful traffic or unauthorized use and action is reasonably necessary to contain the activity, protect customers or the network, or comply with a lawful direction. It also permits termination for confirmed unlawful use or misuse that continues after corrective action, with notice as soon as practicable unless legally prohibited.

The wholesale provider's publicly filed plan states that its service agreements prohibit illegal use and permit blocking or termination for fraudulent, illegal, improper, or unauthorized use, including blocking numbers, trunks, or a customer account.

### 6. Investigation, account security, and suspension

Eric L. Johnson handles reports involving suspected misuse of CTG customers' voice service. CTG evaluates the source, type, and details of the report when determining its response. For an abuse notice from the wholesale provider identifying a customer account and suspected calls, CTG will use the following process:

**1.** Contact the client to determine whether anyone has had access to the client's account or physical phones.

**2.** If the client cannot account for the activity, reset the relevant account passwords and ensure that two-factor authentication is enabled on accounts that support it.

**3.** Notify the wholesale provider of the actions taken and request monitoring to determine whether the issue has been resolved.

**4.** If the calls continue, suspend service on the extension or extensions from which the calls originate. If the issue is broader, suspend service for the customer account as a whole.

### 7. Traceback cooperation

CTG commits to respond fully within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, with response timing determined under 47 CFR Section 64.1200(n)(1). CTG commits to cooperate with those entities in investigating and stopping illegal robocallers that use its service to originate calls.

Eric L. Johnson is responsible for receiving and responding to these requests. CTG will help identify the customer and source of the specified calls and obtain assistance from its wholesale provider where needed.

**Responsible person:** Eric L. Johnson, Owner, Operations
775-636-8378, extension 101 | eric@credocomputers.com