

## **ROBOCALL MITIGATION PLAN**

*Concord III, LLC d/b/a Concord Technologies*

*Revised September 2026*

### **I. REGULATORY BACKGROUND**

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires voice service providers to implement STIR/SHAKEN authentication on Session Initiation Protocol (“SIP”) traffic on carrier networks as well as to implement a Robocall Mitigation Plan (“RMP”) covering non-SIP Time Division Multiplexing (“TDM”) traffic. Because Concord III, LLC d/b/a Concord Technologies (“Concord”) sells facsimile services to end user business customers and facsimile service resellers, the Federal Communication Commission (“Commission”) may consider Concord a voice service provider under the TRACED Act.

The Commission essentially defines robocalls as telephone calls with a pre-recorded or artificial voice message delivered through automated dialing technology. Concord sells a document fax delivery service with no voice component and different protocols. Unlike robocalls, which carry voice signals, fax platforms and machines use a specific frequency to transmit data. Fax machines by design deliver and receive fax signals, not standard voice calls. Accordingly, when providing outbound fax delivery service for customers, Concord transmits data over the underlying network facilities of telecommunications carriers and no pre-recorded or artificial voice recordings. Moreover, fax machines on the receiving end of Concord’s services will not interpret a pre-recorded or artificial voice message (robocall) intended for a telephone; meaning, an inbound robocall will not play the recorded message on a fax line to a fax customer. Without regard to whether the Commission considers the delivery of fax messages voice calls, Concord subjects all calls (faxes) originating on the Concord network to a robocall mitigation program meeting or exceeding Commission requirements.

The Commission designed STIR/SHAKEN obligations to authenticate caller ID for voice telephone calls and not fax transmissions. In the event the Commission considers Concord a voice service provider for purposes of STIR/SHAKEN implementation, the Commission grants Concord a continuing extension for implementing STIR/SHAKEN authentication for TDM traffic, and traffic carried over networks in which Concord lacks control of the network infrastructure necessary to implement the STIR/SHAKEN framework pursuant to 47 C.F.R. §64.6301 (a). In order to qualify for the extension, Concord must comply with Commission rules applicable to such portions of the Concord network subject to extension. To this end, Concord submits this RMP to the Robocall Mitigation Database describing and confirming practices, policies, and procedures to mitigate unlawful robocalling. Concord reserves the right to modify, add, delete, or otherwise alter any of the policies and procedures described herein at any time as it deems appropriate to reflect its business, its capabilities, its needs, and its legal obligations.

This RMP describes specific reasonable measures that Concord implements on all calls to detect, prevent, and mitigate illegal robocalls including the following:

- (1) Concord's specific reasonable steps to avoid originating illegal robocall traffic;
- (2) Concord's commitment to full and timely response to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group ("ITG"), and to cooperate with such entities in investigating and stopping illegal robocallers using Concord's service to originate calls;
- (3) Concord's intent to participate in industry tradeshows, groups, or consortiums, working to strengthen efforts to combat unlawful robocalling, and additional call verification and authentication solutions;
- (4) A description of affirmative, effective measures Concord takes to prevent new and renewing customers from using Concord's services to originate illegal calls;
- (5) A description of Concord's know-your-upstream-provider procedures; and
- (6) A description of the call analytics systems Concord uses to identify and block illegal traffic.

## **II. EFFORTS TO AVOID ORIGINATING ILLEGAL ROBOCALLS**

Concord currently delivers facsimile traffic relying upon the TDM networks of underlying telecommunications carriers, SIP trunks or a combination of SIP and TDM. Concord's transition to a digital cloud-based, high-performance network SIP solution for Concord customers relies upon developing proprietary software seamlessly replacing traditional copper voice lines in the network. Concord's meaningful investments in software technology, equipment, and resources prevents the delivery of unlawful facsimile in accordance with the Telephone Consumer Protection Act ("TCPA"), while contemporaneously combatting the possible sending of illegal robocalls consistent with rigorous regulatory and compliance requirements. As part of its RMP, Concord employs the following affirmative measures designed to effectively prevent customers from using Concord's services to originate robocalls and to minimize the impact illegal and unwanted robocalls may cause for consumers and businesses:

### **A. General Terms and Conditions**

Concord requires customers to represent and warrant that they will not utilize Concord's services for any illegal purposes in the contracts they sign with Concord. Concord's contracts prohibit customers from utilizing the service for any illegal, fraudulent, objectionable and/or unauthorized manner, reserving to Concord the sole and absolute right to deny, restrict or immediately suspend or terminate service if the use of the service by the customer, or any end user, either violates the Concord contract or law.

Concord's terms and conditions permit Concord, without notice, to discontinue, block or suspend services if necessary to prevent an end user from using services for illegal purposes. Concord will block or suspend the service of any customers originating unlawful robocalls through Concord's services. Concord's RMP includes an increasing investment in resources over time to further strengthen adherence to compliance requirements by customers.

## **B. Measures to Prevent New and Renewing Customers from Originating Illegal Calls**

In compliance with the Commission's requirements, Concord has implemented the following procedures:

- **Pre-Activation Screening.** Before activating service for any new customer, Concord conducts a review of the prospective customer's identity, business purpose, and intended use of Concord's facsimile services. Concord's screening procedures include the use of publicly available databases and research tools, including LinkedIn, ZoomInfo, and general internet searches, to verify the prospective customer's business identity, operational history, and commercial legitimacy. Concord cross-references available datapoints to confirm consistency before activating service. Concord's finance team plans to implement additional enhanced verification checks for new customer onboarding in the near term.
- **Contractual Obligations.** All new customer agreements and renewals incorporate Concord's current terms and conditions, which expressly prohibit the use of Concord's network for illegal robocalling, spoofing, or any activity that violates the TCPA or applicable state and federal law. Customers must affirmatively acknowledge and agree to these obligations at the time of contract execution and renewal.
- **Volume and Use-Case Assessment.** Concord evaluates expected traffic volumes and use patterns at onboarding. Prospective customers requesting unusually high volumes or exhibiting usage patterns inconsistent with legitimate facsimile delivery may be subject to enhanced due diligence, additional documentation requirements, or denial of service.
- **Ongoing Monitoring of Renewed Accounts.** At the time of contract renewal, Concord reviews the customer's historical traffic patterns, complaint history, and compliance with contractual obligations. Concord reserves the right to decline renewal or impose additional conditions on customers whose usage patterns raise compliance concerns.

## **C. Third Party Analytics and Monitoring**

Concord works with underlying providers and consultants to support the deployment of systems to detect potential robocall and other unlawful activity relating to transmitting faxes. Concord receives and continuously monitors analytics from its underlying network providers, including

statistics such as average call duration, ASR, and call count carrier/consumer reports. Concord relies upon such call analytics and internal processes developed over the last twenty-five (25) years to identify prohibited conduct and block illegal traffic.

#### **D. Traffic Reports, Industry Information and Monitoring**

Concord captures Call Detail Records (“CDR”) in an Elastic database for monitoring and analysis purposes. Concord uses real-time dynamic traffic analytics and continuously monitors reports generated by CDR and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints that may catch potential unlawful robocalling. Although no evidence exists suggesting Concord in any way originates illegal robocall campaigns, Concord maintains the contractual right to take the action it deems necessary to eliminate robocalls.

#### **E. Internal Controls and Analytics**

Concord’s internal analytics and processes use proprietary intellectual property to analyze data points, including calling patterns, call durations, and connectivity rates, to detect and mitigate suspicious activity. The systems enable Concord to proactively block irregular traffic, and raise alerts for further investigation, thereby ensuring network integrity. Specifically, Concord’s operations team reviews and monitors the following indicators of potentially illegal traffic:

- Anomalous spikes in outbound call volume from individual customer accounts or number ranges;
- Unusually short call durations or abnormally low answer-seizure ratios indicative of automated dialing;
- Sequential or patterned dialing to consecutive telephone numbers;
- High volumes of calls to numbers on Do-Not-Call registries or to unassigned NPA-NXX codes;
- Origination of traffic using caller ID numbers not assigned to or authorized for the originating customer; and
- Sudden changes in traffic patterns inconsistent with a customer’s historical usage profile.

When Concord detects these or other indicators of suspicious activity, Concord’s operations team initiates an investigation, which may result in temporary suspension of the customer’s outbound traffic, a request for additional documentation, or permanent termination of service.

## F. Telephone Number Validation

Concord assigns telephone numbers to out-pulse in the call stream with each fax transmission. Unless the customer ports a telephone number from another fax service provider to use with the fax delivery service, Concord owns the out-pulse telephone numbers. Concord's fax platform will only out-pulse telephone numbers Concord associates with a customer. Through this process Concord verifies the association of the customer with telephone numbers appearing in the call stream.

## III. CUSTOMER VETTING

Concord maintains a customer vetting process to meet "Know Your Customer" ("KYC") obligations. Through Concord's KYC customer process, Concord understands the nature, need, activities, and reputation of its new and existing direct customers. Identifying and understanding customers through this KYC vetting process authenticates the customer connection with the caller ID accompanying each fax delivery, diminishing the opportunity to use Concord's network for spoofed or illegal traffic. Concord's KYC procedures include, at a minimum, the following elements:

- **Identity Verification.** Concord verifies the legal identity of each new customer, including business name, address, authorized contact persons, and tax identification or registration information as applicable.
- **Business Purpose Review.** Concord evaluates the prospective customer's stated business purpose and intended use of facsimile services to confirm consistency with legitimate commercial activity.
- **Caller ID Association.** The KYC process authenticates the customer's connection with the caller ID numbers accompanying each fax delivery, reducing the opportunity to use Concord's network for spoofed or illegal traffic.
- **Ongoing Due Diligence.** Concord conducts periodic reviews of existing customer accounts, including traffic pattern analysis and complaint monitoring, to identify changes in behavior that may indicate misuse of the network.

## IV. KNOW YOUR UPSTREAM PROVIDER

The Commission's directives require voice service providers to describe know-your-upstream-provider procedures designed to mitigate illegal robocalls. An "upstream provider" in this context refers to an entity that sends voice traffic to a provider for transmission or termination. Concord operates exclusively as an originating provider of outbound facsimile traffic and does not currently receive inbound voice traffic from upstream carriers or providers for transmission or termination. Accordingly, Concord has no upstream provider relationships to which the Commission's know-your-upstream-provider requirements presently apply.

Notwithstanding the foregoing, in the event Concord enters into interconnection or service arrangements under which it receives inbound voice traffic from upstream providers, Concord commits to implementing the following measures:

- **Carrier Qualification.** Before entering into an interconnection or service agreement with an upstream carrier, Concord will verify that the carrier maintains an active filing in the Robocall Mitigation Database and has not been the subject of removal by the Commission's Enforcement Bureau.
- **Contractual Protections.** Concord will require that interconnection and service agreements with upstream providers include provisions requiring cooperation with traceback investigations, compliance with applicable robocall mitigation rules, and the right to terminate the agreement in the event of noncompliance.
- **Traffic Monitoring.** Concord will monitor inbound traffic from upstream providers for anomalies, including unusual call volumes, short-duration calls, and patterns consistent with illegal robocalling. When suspicious traffic patterns are identified, Concord will work with the upstream provider to investigate and, if necessary, block the offending traffic.
- **Periodic Review.** Concord will periodically review the RMD filings and compliance status of any upstream providers to confirm that they remain in good standing with the Commission.

## V. ACTIVE INTERFACE WITH UNDERLYING PROVIDERS

Concord depends upon the physical networks of underlying providers to sell fax delivery services over physical TDM lines and SIP channels to its customers. Concord lacks control of the network infrastructure supporting call termination, call origination, telephone numbers needed to fully implement the STIR/SHAKEN framework on the network supporting Concord's entire customer base, relying in most instances upon underlying providers in obtaining the highest attestation levels possible with all calls. Concord and its underlying network providers lead the industry development of call authentication technology and commit to fully implementing STIR/SHAKEN.

## VI. COMMITMENT TO RESPONDING TO TRACEBACK REQUESTS

Concord fully commits to responding within twenty-four (24) hours to all traceback requests from the Commission, law enforcement, and the ITG. Concord will cooperate with such entities in investigating and stopping illegal robocallers using Concord services to originate calls.

Concord sells facsimile services to end user business customers and facsimile service resellers. At no time since organizing in 2001 has Concord been notified by any regulatory agency that it has been suspected of or being investigated for carrying illegal robocalls originating on

Concord's network. Concord has not received notice of any existing Commission, law enforcement, ITG or other regulatory action or investigation involving Concord due to unlawful robocalling or spoofing. No law enforcement or Commission action bars Concord from the Robocall Mitigation Database.

To allow for timely and comprehensive response to traceback requests, Concord maintains and will devote sufficient resources to provide prompt and complete records in response to traceback requests. Concord designates the following individual as the single point of contact for receiving all traceback requests:

Patricia Zonnenberg  
Chief Legal Counsel  
Concord III, L.L.C.  
2025 First Avenue, Suite 800  
Seattle, WA 98121  
(206) 441-3346  
generalcounsel@concord.net

## **VII. ENFORCEMENT AND INVESTIGATION HISTORY**

As required by the Commission's expanded RMD filing requirements, Concord discloses the following regarding its enforcement and investigation history:

- Concord has had no licenses revoked by the Commission and has not been subject to enforcement action by the Commission.
- Concord has not been removed from, or prohibited from filing in, the Robocall Mitigation Database by Commission action.
- Concord has not been the subject of any Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- No law enforcement or Commission action bars Concord from the Robocall Mitigation Database.

In the event of any material change to the foregoing, Concord will update its RMD filing within ten (10) business days of such change, consistent with 47 C.F.R. § 64.6305.

## **VIII. PLAN UPDATES**

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Concord will monitor industry best practices and continuously improve its internal processes to ensure this plan and its systems adapt to this ever-changing issue. In the event of any material change to this plan, Concord will make it available to employees,

consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) business days of such update, consistent with amended 47 C.F.R. § 64.6305(h).

## CERTIFICATION

I, Charles Padgett, Chief Financial Officer of Concord III, L.L.C. (“Concord”), do hereby certify, under penalty of perjury, the following:

- a. Concord exclusively delivers fax messages and no pre-recorded or artificial voice messages.
- b. Concord subjects all calls originating on its network to this Robocall Mitigation Plan consistent with 47 C.F.R. §64.6305 (a).
- c. Any prior certification has not been removed by the Commission action and Concord has not been prohibited from filing in the Robocall Mitigation Database by the Commission.
- d. Concord lacks the control over the necessary infrastructure technology to implement STIR/SHAKEN requirements in its TDM network.
- e. Concord has not been a foreign voice service provider.
- f. Concord business name and primary address follows:

Concord III, L.L.C.  
2025 First Avenue, Suite 800  
Seattle, Washington 98121

- g. Concord operates under the corporate name Concord III, L.L.C., Concord Technologies, Concord IV, L.L.C. and Biscom, Inc.
- h. Concord previously also operated under the name Opero, L.L.C., precursor to Concord IV, L.L.C.
- i. The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues follows:

Name: Patricia Zonnenberg  
Title: Chief Legal Counsel  
Department: Executive  
Address: 2025 First Avenue, Suite 800  
Seattle, WA 98121  
Telephone: (206) 441-3346  
Email: [generalcounsel@concord.net](mailto:generalcounsel@concord.net)

- j. Concord has had no licenses revoked by the Commission and has not been subject to enforcement action by the Commission.
- k. Concord’s role in the call chain remains that of a voice service provider without a STIR/SHAKEN implementation obligation for current service offerings.

- l. Concord has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- m. Concord has not been the subject of a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- n. Concord OCN remains 843K.

Signed by:



38CE7A7FEE9B42B...

Name: Charles Padgett

Title: Chief Financial Officer

Date: 04-Sep-2026 | 5:58 PM PDT, 2026