

# Robocall Mitigation Plan

**CloudPBX Inc. (DBA CORVUM)**

April 2026

FRN: 0031441322

## PURPOSE

CloudPBX Inc. (DBA CORVUM) is committed to minimizing the number of robocalls that originate on its network and to preventing unlawful calls from being transmitted through its services. This Robocall Mitigation Plan (“RMP”) describes: (1) the specific reasonable steps CORVUM takes to avoid carrying or processing illegal robocall traffic; (2) CORVUM’s commitment to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission (“Commission”), law enforcement, and the industry traceback consortium; and (3) CORVUM’s commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use its services to carry or process calls.

## ENTITIES COVERED BY CERTIFICATION

This RMP covers the following entity:

**CloudPBX Inc. (DBA CORVUM) — FRN: 0031441322**

## KNOW YOUR CUSTOMER PROCEDURES

CORVUM provides voice communications services primarily to businesses operating in the legal industry. All prospective customers are required to provide accurate business information during the account setup process. CORVUM conducts manual spot checks to verify customer identity and confirm the legitimacy of the business prior to and during the provision of service. Customers who cannot be verified as legitimate businesses are denied access to CORVUM’s services.

## KNOW YOUR UPSTREAM PROVIDER

CORVUM’s upstream provider in the United States is Bandwidth Inc., which is registered in the Robocall Mitigation Database (“RMD”) with registration number RMD0002564. CORVUM only accepts traffic from upstream providers that are listed in the Robocall Mitigation Database. Bandwidth Inc. maintains its own call analytics monitoring systems for the detection of illegitimate traffic. Should Bandwidth Inc. detect suspicious activity, CORVUM will work directly with them to identify any corresponding account and follow the same process to immediately suspend the account and subsequently terminate the account in accordance with CORVUM’s Terms of Service.

## **CUSTOMER COMPLIANCE WITH ROBOCALLING RULES AND EXISTING LAW**

CORVUM requires all customers to comply with its Terms of Service, which generally prohibit robocalling, automated calling of any kind, or other unlawful calling practices under applicable federal and state law, including the Telephone Consumer Protection Act (“TCPA”) and FCC rules and regulations. Additionally, CORVUM’s services are architected such that caller ID spoofing is not technically possible, further ensuring that customers are unable to engage in one of the most prevalent forms of illegal robocall activity. Any customer found to be in violation of CORVUM’s Terms of Service is subject to immediate suspension and subsequent termination of service if such violation is left uncured.

## **STIR/SHAKEN IMPLEMENTATION**

CORVUM has implemented STIR/SHAKEN throughout its network in full compliance with ATIS standards. All calls originated by CORVUM customers are signed with full (“A”) attestation through CORVUM’s upstream provider, Bandwidth Inc. STIR/SHAKEN uses digital certificates based on common public key cryptography techniques to ensure the calling number of a telephone call is secure, enabling the called party to verify that the calling number is accurate and has not been spoofed.

## **ANALYTICS & MONITORING**

CORVUM actively monitors call traffic across its network for signs of suspicious or illegal activity. CORVUM’s monitoring program includes both call volume threshold analysis and suspicious calling pattern detection. When potentially suspicious activity is identified, CORVUM promptly investigates and takes appropriate action, up to and including immediate suspension of the offending account and eventual termination if left uncured.

## **INCIDENT RESPONSE AND TRACEBACK REQUESTS**

CORVUM commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. When a traceback request is received or a credible complaint is brought to CORVUM’s attention, CORVUM promptly investigates the suspect traffic to determine the call path(s) and whether the traffic is likely to constitute illegal robocalling.

If a customer is found to be engaging in illegal robocalling or any other prohibited calling activity, CORVUM will immediately suspend that customer’s access to its services upon discovery. CORVUM will terminate customer access to its services in accordance with CORVUM’s Terms of Service if Customers are found to be engaging in illegal activities.

In addition to CORVUM’s own monitoring, Bandwidth Inc. also maintains call analytics monitoring systems for the detection of illegitimate traffic. Should Bandwidth Inc. detect suspicious activity, CORVUM will work directly with them to identify the corresponding account and take immediate action as set out above.

## **PRINCIPALS, AFFILIATES, SUBSIDIARIES & PARENT COMPANIES**

CloudPBX Inc. (DBA CORVUM) is a wholly-owned subsidiary of Themis Solutions Inc. (DBA CLIO). Jack Newton is the Chief Executive Officer of CLIO and the sole director of CORVUM,

has no other affiliates or subsidiaries that independently meet the definition of a voice service provider, intermediate provider, or gateway provider.

Neither CloudPBX Inc. (DBA CORVUM) nor any of its principals have been subject to a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

## REVISION HISTORY

| Description | Revision Date |
|-------------|---------------|
| Revision    | April 2026    |