

ROBOCALL MITIGATION PLAN

Cloud Worldwide Services LLC

Submitted pursuant to 47 C.F.R. § 64.6305

Robocall Mitigation Database (RMD) Filing

1. Company Identification

The following information identifies the filing entity:

Legal Name: Cloud Worldwide Services LLC ("CWS")

FRN: 0037162112

Filer ID: 837961

OCN: 066M

Principal Place of Business: Spain (European Union)

Website: www.cloudworldwideservices.com

Cloud Worldwide Services LLC is a New York-incorporated Software-as-a-Service (SaaS) provider and the U.S. operating entity of Cloud Worldwide Services S.L. (Spain), specializing in cloud communication services for business customers. CWS operates infrastructure primarily on Amazon Web Services (AWS) and Microsoft Azure and serves clients across multiple jurisdictions. CWS is registered with the FCC as part of its commitment to compliance with applicable U.S. telecommunications regulations, specifically in connection with the STIR/SHAKEN framework and the Robocall Mitigation Database requirements.

2. Service Description — eComFax

CWS provides a cloud-based Fax over IP (FoIP) service commercially known as eComFax. The service is designed exclusively for business-to-business and business-to-individual secure document communications. eComFax is not a voice telephony service, a robocalling platform, or a telemarketing solution.

Key technical and operational characteristics of eComFax include:

- Cloud-native SaaS architecture: eComFax operates entirely as a cloud-based application. There is no on-premise hardware dependency for the end customer.
- Fax over IP (FoIP) technology: The service converts documents (e.g., PDF, TIFF) into fax transmissions using T.30/T.38 protocols over IP networks, enabling interoperability with traditional Public Switched Telephone Network (PSTN) numbering.

- Email-to-Fax / Fax-to-Email conversion: Users send and receive fax documents via standard email interfaces or API integrations, with the platform handling protocol conversion transparently.
- Information Service classification: eComFax processes, transforms, and stores information, placing it squarely within the FCC's definition of an "Information Service" as defined in 47 U.S.C. § 153(24). Revenues are reported on Line 418.3 of FCC Form 499-A.
- Business-oriented use: The service is targeted at regulated industries requiring secure document exchange, such as healthcare, legal, and financial sectors. It is not marketed or configured for high-volume unsolicited communications.
- No voice calling capability: eComFax does not originate, transit, or terminate voice calls. The PSTN interconnection is limited strictly to facsimile transmission signals.

Given the nature of eComFax as a document-transmission Information Service with limited PSTN interoperability, the volume of calls (fax sessions) originated is low and the risk profile associated with illegal robocalling is minimal. CWS does not provide mass voice broadcasting, predictive dialing, or any service that could facilitate unsolicited robocall campaigns.

3. Customer Verification Measures

CWS applies reasonable due diligence procedures prior to activating eComFax services for any customer. These procedures are designed to ensure that the service is used for legitimate business communications and to prevent misuse.

3.1 Business Identity Validation

- Customers are required to provide verifiable business information, including legal name, country of incorporation or registration, and contact details of a responsible representative.
- For customers requiring PSTN-connected numbers, CWS or its upstream providers conduct additional verification of the intended use case and business legitimacy.
- CWS does not activate services for anonymous accounts or customers who cannot demonstrate a legitimate business purpose.

3.2 Contractual Controls

- All customers must accept CWS's Terms of Service and Acceptable Use Policy (AUP) prior to service activation. These documents explicitly prohibit unlawful robocalling, caller ID spoofing, and any other fraudulent use of the service.
- The contractual framework provides CWS with the legal basis to suspend or terminate service in the event of policy violations.

3.3 Use-Case Assessment

- CWS evaluates the stated purpose of the service at onboarding. Customers whose use cases are inconsistent with legitimate document transmission (e.g., requests for high-volume outbound call capabilities inconsistent with fax services) are not activated.

4. Traffic Monitoring and Anomaly Detection

CWS maintains internal controls for monitoring the traffic generated through its eComFax service. Given that fax transmission generates a distinct and generally predictable traffic profile, deviations from expected patterns are identifiable through standard monitoring practices.

CWS's traffic monitoring activities include:

- Volume monitoring: CWS monitors session volumes per customer account. Unusual spikes in outbound fax sessions that deviate significantly from historical usage patterns trigger internal review.
- Anomalous pattern detection: CWS reviews traffic for indicators inconsistent with legitimate fax use, including atypical destination number patterns, abnormally short session durations (which may indicate spoofing rather than genuine fax transmission), or attempts to originate traffic toward numbers associated with known fraud or abuse reports.
- Upstream coordination: CWS cooperates with its upstream voice and PSTN interconnection providers to receive alerts or notifications regarding suspicious traffic patterns that may be traced to its customer accounts.
- Internal review procedures: When anomalous activity is identified, CWS conducts an internal review, which may include account-level traffic analysis, customer contact for clarification, and if warranted, suspension of service pending investigation.

These measures are proportionate to the low-risk profile of a fax-only SaaS service. CWS will adjust and enhance its monitoring capabilities as the service scales and as regulatory guidance evolves.

5. Acceptable Use Policy and Anti-Spoofing Commitments

CWS maintains and enforces a formal Acceptable Use Policy (AUP) applicable to all eComFax customers. The AUP expressly prohibits the following:

- Origination, transmission, or facilitation of illegal robocalls as defined under the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227, or any other applicable U.S. or international law.
- Caller ID spoofing or any manipulation of calling party number information with intent to defraud, deceive, or cause harm, in violation of the Truth in Caller ID Act, 47 U.S.C. § 227(e).
- Use of CWS services for phishing, vishing, smishing, or any other form of fraud or social engineering.

- Transmission of unsolicited commercial facsimiles in violation of the TCPA or equivalent regulations.
- Any use of the service that violates applicable federal, state, or international telecommunications laws and regulations.

CWS's anti-spoofing commitment extends to ensuring that the calling party numbers associated with eComFax transmissions are valid, allocated numbers associated with legitimate accounts. CWS does not permit customers to present arbitrary or unverified numbers as the originating identifier in fax sessions that interact with the PSTN.

6. Mitigation Measures and Enforcement Actions

In the event that CWS detects or receives credible information regarding suspected abusive or illegal use of its eComFax service, the following response procedures apply:

Step 1 — Initial Investigation:

CWS conducts an internal review of the relevant account's traffic data, contract documentation, and any available contextual information to assess the nature and scope of the suspected violation.

Step 2 — Traffic Restriction:

Where there is a reasonable basis to believe that abusive traffic is being generated, CWS may immediately restrict or throttle the relevant account's outbound traffic while the investigation proceeds, without prior notice if the risk of harm is considered imminent.

Step 3 — Account Suspension:

If the investigation confirms a violation of the AUP or applicable law, CWS may suspend the customer's account and disable access to all services, pending resolution.

Step 4 — Service Termination:

In cases of confirmed serious violations, CWS will permanently terminate the customer's account and retain records of the violation in accordance with applicable data retention obligations.

Step 5 — Regulatory Referral:

Where the violation may constitute a criminal offense or where regulatory reporting is required or advisable, CWS will cooperate with and, where appropriate, proactively notify relevant authorities, including the FCC.

7. Complaint Handling and Traceback Cooperation

CWS is committed to responding promptly and cooperatively to complaints and traceback requests related to its services.

7.1 Complaint Intake

CWS maintains a designated point of contact for receiving complaints related to potential unlawful use of its services. Complaints may be submitted by customers, third parties, upstream or downstream operators, or regulatory authorities. Upon receipt, complaints are logged, acknowledged, and reviewed within a reasonable timeframe.

7.2 Traceback Cooperation

CWS will cooperate fully with traceback requests submitted through the USTelecom Industry Traceback Group or equivalent mechanisms recognized by the FCC. Upon receipt of a valid traceback request:

- CWS will review its internal records to identify the customer account associated with the traffic in question.
- CWS will provide a response within the timeframe specified in the traceback request, or as otherwise required by applicable FCC rules.
- CWS will share available information about the relevant account and traffic, subject to applicable privacy and data protection obligations under Spanish and EU law (including the GDPR).

7.3 Regulatory and Law Enforcement Cooperation

CWS will respond to lawful requests for information from the FCC, the Department of Justice, and other competent U.S. or international authorities regarding traffic potentially associated with illegal robocalling or related fraud. The designated compliance point of contact for such inquiries is compliance@cloudwws.com. CWS will ensure that requests received at this address are routed promptly to the appropriate internal personnel.

8. STIR/SHAKEN Implementation Status

CWS acknowledges the FCC's STIR/SHAKEN call authentication framework established pursuant to the TRACED Act (Pub. L. 116-105) and implemented through 47 C.F.R. Part 64, Subpart CC.

CWS's current status with respect to STIR/SHAKEN is as follows:

- eComFax is a Fax over IP (FoIP) Information Service, not a traditional voice service. The technical architecture of FoIP transmissions, which use T.30/T.38 protocols, is distinct from SIP-based voice calling and does not natively support STIR/SHAKEN call signing in the manner applicable to interconnected VoIP voice services.

- CWS is currently evaluating the specific applicability of STIR/SHAKEN obligations to its FoIP service model, including the extent to which the service falls within the scope of providers required to obtain Service Provider Codes (SPC tokens), Secure Telephone Identity (STI) certificates, and to operationally sign calls.
- Pending the completion of this evaluation and any applicable regulatory clarification, CWS is implementing reasonable robocall mitigation measures as described in this Plan as an alternative to full STIR/SHAKEN implementation, consistent with the options available to providers under 47 C.F.R. § 64.6305(b).
- CWS will continue to monitor FCC guidance, including any further rulemaking regarding non-voice services and FoIP, and will implement STIR/SHAKEN or equivalent authentication measures as and when technically feasible and legally required.

CWS does not claim full STIR/SHAKEN compliance at this time. This Plan reflects CWS's current robocall mitigation posture in good faith, consistent with the applicable regulatory framework for its service type and operational scale.

9. General Compliance Commitment

Cloud Worldwide Services, LLC is committed to operating its eComFax service in full compliance with applicable U.S. telecommunications law and FCC regulations, including the requirements of the TRACED Act, the Truth in Caller ID Act, the TCPA, and all relevant FCC orders and rules relating to robocall mitigation and call authentication.

CWS will review and update this Robocall Mitigation Plan as its services evolve, as the regulatory framework develops, and as required by the FCC. CWS will promptly notify the Robocall Mitigation Database of any material changes to the information contained herein.

CWS does not permit, facilitate, or knowingly enable the use of its services for illegal robocalling, caller ID spoofing, or any other fraudulent communications activity. CWS is committed to being a responsible participant in the U.S. telecommunications ecosystem and to cooperating proactively with industry and regulatory efforts to combat illegal robocalls.

Signed:

Name: ENRIQUE VAÑÓ MARTINEZ
Title: CISO
Date: 14/05/2026
On behalf of: Cloud Worldwide Services LLC

