

J2 Web Services, Inc.

Robocall Mitigation Plan

Updated: March 2026

I. Introduction

As part of J2 Web Services's ("J2") submission to the Robocall Mitigation Database, pursuant to section 64.6305 of the Commission's rules, this document outlines (1) the reasonable steps J2 has taken to avoid originating illegal robocall traffic; (2) J2's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium; and (3) J2's commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use J2's service to originate calls. This Robocall Mitigation Plan ("RMP") serves to provide the Commission with specific details regarding J2's mitigation strategy.

A. Company Summary

J2 is a Delaware corporation and wholly owned subsidiary of Ziff Davis, Inc., a publicly traded company (NASDAQ: ZD). Information regarding Ziff Davis and J2, including principal management, may be found at www.ziffdavis.com. A list of subsidiaries of Ziff Davis is included in its SEC Form 10-K available at <https://investor.ziffdavis.com/financials/sec-filings/default.aspx>.

J2 provides various voice and communications services. Related to this Robocall Mitigation Plan, J2's brands include Onebox, eVoice, and Line2, each of which provides some form of voice service in all fifty states. J2 provides voice services to a broad range of enterprise customers across its IP and TDM networks as an interconnected and non-interconnected Voice over Internet Protocol ("VoIP") provider.

B. STIR/SHAKEN Compliance

J2 is a voice service provider and has implemented the STIR/SHAKEN authentication framework network-wide and calls it originates on its network are compliant with 47 C.F.R. § 64.6301(a)(1) and (2). J2 has developed its own tools to monitor for anomalous activity, including attempts to misuse direct-inward dialing ("DID") configurations and also applies the mitigation controls described in this RMP to address any suspected illicit robocalls or unauthorized caller ID spoofing.

For all calls that J2's users originate on its network, J2 authenticates (signs) those outbound SIP calls using a certificate issued to J2 and assigns attestation levels consistent with the STIR/SHAKEN technical standards. J2 relies on STIR/SHAKEN authentication, contractual restrictions, and the monitoring and investigation controls described in this RMP to prevent and remediate misuse of its network. J2 also works with its upstream carrier partners on mitigation for DID traffic and can determine whether calls entering its network environment are signed or unsigned.

II. Elements of the Company's Robocall Mitigation Plan

The Company's Robocall Mitigation Plan contains the following elements:

1. Contractual Provisions to Mitigate Origination of Illegal Robocalls
2. Know Your Upstream Provider Procedures
3. Know Your Customer Procedures
4. Analyzing and Monitoring Traffic Patterns
5. Investigating Suspicious Activity
6. Employee Training

A. Contractual Provisions to Mitigate Origination of Illegal Robocalls

Voice service customers of J2 are subject to robust terms and conditions that include provisions that (1) obligates customers not to use J2's services for unlawful purposes; (2) expressly prohibits conduct specifically associated with illegal robocalls; and (3) preserves J2's right to terminate customers for violations of the law. J2 maintains separate agreements for its eVoice, Onebox, and Line2 services, however, the agreements generally include similar terms and conditions. For purposes of this Robocall Mitigation Plan, J2 references its eVoice Customer Agreement in the narrative, and highlights similar terms and conditions for its Onebox and Line2 services in the footnotes.¹

For all of its eVoice customers, J2 maintains a "Customer Agreement"² which includes robust legal compliance and termination clauses. With respect to the former, the Customer Agreement requires all J2 eVoice customers to comply with "all applicable local, state, national and international laws and regulations."³ Among other things the Customer Agreement expressly prohibits eVoice customers from using J2's services: 1) for any "illegal purposes;"⁴ 2) to

¹ The Onebox customer agreement is available at: <https://www.onebox.com/signup/terms-popup> ("Onebox Customer Agreement"); and the Line2 customer agreement is available at: <https://www.line2.com/terms-of-service/> ("Line2 Customer Agreement").

² See eVoice website, Customer Agreement, available at: <https://www.evoice.com/customer-agreement> (visited February 12, 2026) ("eVoice Customer Agreement").

³ eVoice Customer Agreement, Section 7(d). See also Onebox Customer Agreement, Section 11 (Prohibited Conduct); Line2 Customer Agreement, Section 1 (Acceptable Use) (stating that use of the Line2 service is limited to "a manner consistent with all applicable laws and regulations.").

⁴ *Id.*, Section 7(d)(2). See also Onebox Customer Agreement, Section 11 (Prohibited Conduct), para. 2; Line2 Customer Agreement, Section 1 (Unlawful Use Prohibited).

“transmit misleading or inaccurate caller identification information,”⁵ or 3) “with the intent to defraud, cause harm, or wrongfully obtain anything of value.”⁶

The Customer Agreement also includes provisions that expressly prohibit the use of J2’s eVoice service to transmit any type of spam messages—including voice, fax and text messages.⁷ Specifically, the Customer Agreement expressly prohibits eVoice subscribers from transmitting “any material that encourages conduct that could constitute a criminal offense, give rise to civil liability or otherwise violate any applicable local, state, national or international law or regulation,” to include “fax, text message, or voice ‘spam’ or other unsolicited marketing message.”⁸

Finally, with respect to termination, J2 also retains the right to “immediately terminate or suspend” a customer’s eVoice service “at any time, with or without cause, upon notice.”⁹ Further, the Customer Agreement reserves the right for J2 to “terminate any account if [J2] believe[s] unreasonable usage has occurred on such account or if the services are used in a manner that is not permitted by” the Customer Agreement.¹⁰

B. Know Your Customer Procedures

J2 has no upstream providers so it does not have any procedures to confirm such. For its customers, J2 employs a large number of automated checks to determine if an account signup is legitimate during its onboarding process. New signups will either be approved, automatically denied, or tentatively approved. J2 employees will review tentatively approved signups and

⁵ *Id.*, Section 7(d)(10). *See also* Onebox Customer Agreement, Section 11 (Prohibited Conduct), para. 14; Line2 Customer Agreement, Section 1 (Acceptable Use) (prohibiting users from “creating a false Caller ID identity (‘ID spoofing’) ... or otherwise attempting to mislead others as to the identity of the sender or the origin of any communication made using the services.”)

⁶ *Id.* *See also* Onebox Customer Agreement, Section 11 (Prohibited Conduct), para. 14; Line2 Customer Agreement, Section 1 (Acceptable Use) (prohibiting use of the service by subscribers that is “deceptive in any way, such as an offer to sell fraudulent goods or contains an impersonation of any person or entity or misrepresents an affiliation with a person or entity.”).

⁷ *See e.g., id.*, Section 7(d)(a). *See also* Onebox Customer Agreement, Section 11 (Prohibited Conduct), para. 7; Line2 Customer Agreement, Section 1 (Acceptable Use) (prohibiting any use of the service by subscribers that “constitutes unsolicited or unauthorized advertising, including . . . Short Message Service (SMS), Multimedia Messaging Service (MMS), Line2 messaging, voicemail, or faxes (‘spamming’), or otherwise sending junk or bulk . . . voicemail or faxes.”).

⁸ *Id.* *See also* Onebox Customer Agreement, Section 11 (Spam); Line2 Customer Agreement, Section 1 (Acceptable Use).

⁹ *Id.*, Section 13(2). *See also* Onebox Customer Agreement, Section 12 (Disclaimer of Warranties); Line2 Customer Agreement, Section 1 (Termination or Suspension of Account).

¹⁰ *Id.* *See also* Onebox Customer Agreement, Section 16 (Termination or Suspension); Line2 Customer Agreement, Section 1 (Termination or Suspension of Account) (permitting termination of account for “any reason.”).

deactivate any accounts that are determined to be illegitimate. J2 utilizes the following processes, systems and techniques to determine the approval/denial status of new accounts:

- Require two-factor authentication for online signups;
- Leverage machine learning algorithms developed by J2's payment processors to identify suspicious "personas;"
- Leverage fraud signup rules developed by J2's payment processors (including Worldpay and Paymentech) to further identify potential fraudulent signups;
- Leverage velocity filters to prevent excessive account signups using the same credit card and temporarily block signups following multiple failed registrations with the same credit card token;
- Maintain blacklists for suspect credit card tokens, email addresses, IP addresses and domain names;
- A valid email address is required during signup, and it is verified using a third-party validation service to ensure its authenticity and deliverability;
- Prohibit free trials and instead use 30-day moneyback guarantee;
- Prevent use of services if pre-authorization on credit card fails;
- Prevent use of services by signups from certain countries; and
- Prevent use of services based on number of credit cards, addresses and email addresses on an account.

C. Analyzing and Monitoring Traffic Patterns

J2 also has policies and procedures governing the analysis and monitoring of its outbound network traffic. Consistent with industry practices, J2 analyzes network traffic originating from its network in order to identify and monitor patterns consistent with illegal robocalls.

As part of its analysis and monitoring of network traffic, J2 maintains a Network Operations Center ("NOC") that provides continuous oversight and monitoring of J2's voice service operations. J2's NOC is staffed with network engineers, database administrators, and system administrators. Much of J2's fraud detection is automated and requires limited manual intervention. In the event of a fraud report, appropriate personnel from customer service, finance and/or operations take action to investigate and if needed disable the offending account.

J2 uses internal automated analytics and other controls to review call data and detect patterns that may be consistent with illegal robocalls or related fraud. Activity flagged by these internal automations is escalated to J2's internal fraud team for review and, where appropriate, remediation. J2 does not use a third-party call analytics vendor to analyze its call data for purposes of robocall mitigation.

For accounts that are ultimately approved and allowed to use J2's services, J2 continues to monitor for fraud and abuse of its systems through a variety of automated checks. These automated checks will either trigger review of the account by J2's dedicated fraud prevention team, or automatic shutdown of the account. Some of these automated checks are listed below:

- If an account of any age exceeds a threshold number of outbound calls in a defined time period, it is automatically shut down;
- If an account of any age exceeds a threshold number of SMS/MMS messages in a defined time period, the messages exceeding the threshold number are blocked, and the account is flagged for review;
- If an account less than one day old exceeds a threshold number of calls in a defined time period for the same ANI, it is automatically shut down;
- If an account less than three days old exceeds a threshold number of hours of calls in a defined time period, it is automatically shut down. A second threshold exists for accounts less than thirty days old;
- If a user on an account less than three days old exceeds a certain number of calls in a defined time period, it is automatically shut down. If an account less than three days old exceeds a certain number of calls across all users on an account in a defined time period, it is sent for review;
- If an account less than thirty days old exceeds a threshold number of click-to-call calls to the same number in a defined time period, it is automatically shut down;
- If an account generates 20 or more Click-to-Call (“C2C”) within a 30-minute window, an alert is triggered to the Fraud team and the account is flagged for review;
- If an account less than thirty days old exceeds a threshold number of international calls in a defined time period, it is automatically shut down;
- If an account less than thirty days old exceeds a threshold dollar amount billed for international calls, it is automatically shut down. A second threshold exists for accounts less than ninety days old that also results in automatic shutdown. A third threshold exists for accounts of any age that results in review of the account;
- If an account of any age exceeds a threshold number of Click-to-Call (“C2C”) calls in a defined time period, it is automatically shut down; and
- If an account of any age exceeds a threshold number of SMS/MMS messages in a defined time period, it is automatically shut down. Accounts that send SMS/MMS messages with certain words in them that are likely to be fraud-related are sent for review.

D. Investigating Suspicious Activity

J2 also monitors network usage by its subscribers and initiates investigations where necessary and appropriate. These efforts include identifying suspicious network activity, receiving automatic alerts associated with such traffic, and distinguishing instances of fraud from honest customer usage. J2 also uses AI and keyword matching to flag accounts. Based on the outcome of an investigation, J2 staff will also take appropriate remediation measures that include resolving

suspected instances of fraud through measures that range from disabling of accounts to termination of subscribers.

E. Employee Training

Finally, J2 employs individuals trained in responding promptly to government inquiries and individuals knowledgeable on identifying the hallmarks of suspicious robocall traffic. Many of these employees retain prior training relevant to the investigation of fraudulent activity on J2's network. J2 will also share the Robocall Mitigation Plan with relevant individuals, who will be required to acknowledge their review and understanding of the plan.

III. Prior Two-Year Regulatory Action / Investigation Disclosure

Pursuant to 47 C.F.R. § 64.6305(d)(2)(iv), J2 Web Services, Inc., and any entity for which J2 shares common ownership, management, directors, or control, has not been the subject, at any time in the prior two years, of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to illegal robocalling or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

IV. Responding to Traceback Requests and Cooperating in Investigating and Stopping Illegal Robocallers

J2 is committed to ensuring that its network is not used for the origination, termination, or routing of unwanted or illegal robocalls. Consistent with 47 C.F.R. § 64.6305(a)(2), J2 commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use J2's service to originate calls. As part of this commitment, J2 will take the necessary steps to effectively mitigate illegal traffic when the company receives actual written notice of such traffic from the FCC through the Enforcement Bureau and will comply with the requirements of any such notice, consistent with the Commission's rules.

To further ensure J2 network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, J2 provides the following name, title, department, business address, telephone number, and email address of the individual within J2 that handles robocall mitigation related issues, as well as responds to traceback inquiries from the FCC, Industry Traceback Consortium, and law enforcement agencies:

Contact Name: Cheryl Lowe
Contact Title: Manager, Fraud
Contact Street: 360 Park Ave. S., 17th floor
Contact City: New York
Contact State and Zip Code: NY 10010
Contact Telephone Number: (888) 799-4913
Contact Email: FCC.email@moz.com (alternate: legal@mozgroup.com)

V. Updating J2's Robocall Mitigation Plan

Consistent with FCC regulations, 47 C.F.R. § 64.6305(d)(5), J2 will update its submission in the Robocall Mitigation Database within 10 business days of any change to the applicable information it must provide in the Robocall Mitigation Database, including its Robocall Mitigation Plan. In addition, consistent with 47 C.F.R. § 64.6305(h), J2 will complete its annual RMD recertification on or before the relevant deadline each year, certifying that the information submitted to the RMD is true and correct.