ROBOCALL MITIGATION PLAN

Pathor Enterprise Ltd. | EmmaVoip | FCC FRN: 0039080676

October 29, 2026

Pathor Enterprise Ltd. (“Pathor”) operates the EmmaVoip application and is developing internet-based voice calling services using an upstream telecommunications provider. This plan sets out Pathor’s approach to identifying and reducing illegal robocalls, deceptive calling, and unauthorized caller ID use. It is intended to support compliance with applicable Federal Communications Commission (“FCC”) requirements, including 47 C.F.R. § 64.6305, and relevant Canadian obligations.

The measures below describe Pathor’s proposed operating policy. Before filing this plan as a statement of current practices, Pathor will verify which controls are implemented and revise any future-tense descriptions accordingly.

Our customers

EmmaVoip will apply customer checks appropriate to the type of account and the risk presented by its calling activity.

Information reviewed may include a customer’s name, verified email address, contact telephone number, location, device or IP information, and payment details where relevant. Business customers may be asked for additional business identity and authorized-user information.

New accounts displaying inconsistent details, unusual registration patterns, or other risk indicators may receive additional review before outbound calling is enabled. Customers will be expected to keep account information accurate. Pathor may request updated verification when an account changes ownership, adds numbers, or displays suspicious usage.

Terms and use

EmmaVoip’s service terms and acceptable-use rules will prohibit illegal robocalls, impersonation, fraudulent solicitations, misleading caller identification, unauthorized automated dialing, and other unlawful or abusive calling.

Customers will be responsible for using the service in accordance with applicable laws and for obtaining any legally required consent.

Where misuse is suspected, Pathor may request an explanation or supporting documentation, impose temporary calling limits, disable outbound service, or terminate the account. Serious or repeated violations may be referred to appropriate authorities or upstream providers.

Telephone number identity (Caller ID)

EmmaVoip will seek to restrict outbound caller ID to numbers assigned through its telecommunications provider or numbers the customer is authorized to use. For externally held numbers, Pathor may require evidence of control, such as a current account statement, verified callback, or other reasonable authorization evidence, before enabling their presentation.

When a customer changes or relinquishes a number, Pathor will seek to remove its calling authorization. Calls presenting invalid, unassigned, or otherwise suspicious caller ID may be rejected, restricted, or investigated.

Blocking and account controls

Pathor intends to apply available application-level and upstream-carrier safeguards to limit suspicious traffic.

Depending on the risk and technical capabilities, these may include account-level calling limits, temporary holds, restrictions on destination ranges, removal of number permissions, and suspension of outbound calling.

Customer reports and upstream-provider warnings will be reviewed to determine whether immediate protective action is needed. Automated blocking or specialized analytics will be represented as active controls only after they have been deployed

and tested.

Traceback

Pathor will cooperate with the FCC, law enforcement, the Industry Traceback Group (“ITG”), and relevant telecommunications providers in tracing suspected illegal calls. Requests will be routed to the designated contact, prioritized, and investigated using available call records and account information.

Pathor will aim to provide a substantive response within 24 hours after receiving a traceback request, subject to the information reasonably available and applicable legal requirements. The response may identify the originating account, relevant calling number, timestamps, and the upstream provider involved. Relevant records will be preserved when an investigation is opened, and confirmed misuse will prompt corrective action.

Monitoring

Pathor intends to review available call-detail records, account activity, customer complaints, and notifications from its upstream provider for indications of unlawful or abusive calling. Indicators may include:

- Unusually high calling volumes or rapid bursts from a single account.
- Multiple simultaneous calls, repeated very short calls, or unusually low answer rates.
- Sequential dialing or repeated calls to large groups of numbers.
- Abrupt changes in a customer’s normal usage, geography, or destinations.
- Repeated complaints, rejected calls, or warnings concerning caller ID misuse.

Potentially suspicious activity will be assessed in context. Pathor may contact the customer, request additional verification, review relevant records, and restrict service while the matter is investigated. Monitoring tools, review frequency, and alert thresholds will be documented as they become operational.

Records and program review

Pathor intends to maintain appropriate records of customer verification, number authorization, call activity, complaints, and investigative actions, subject to applicable privacy and retention obligations. The company will review this plan when material changes occur to its calling services, network arrangements, risk controls, or regulatory obligations.

Operational responsibility rests with Pathor Enterprise Ltd.; the contact below receives compliance and traceback correspondence.

Contact

Pathor Enterprise Ltd.

EmmaVoip | FCC FRN: 0039080676 2914 Lake Shore Blvd W, Toronto, ON, M1L0B3, Canada Designated contact: Ash Rahman Email: support@emmavoip.net