

Robocall Mitigation Program Description

Company: Pet Technologies, Inc.

Doing Business As: Ringable / Ringable.me

FCC FRN: 0037640786

Contact Name: Irvine Pascual

Contact Email: bpascual@inmotiongroup.com

Contact Phone: 248-585-7115 Ext 202

Filing Date: 12/1/2025

1. Company Overview

Pet Technologies, Inc. d/b/a Ringable.Me (“Ringable”) is a U.S.-based interconnected VoIP provider offering a child- and family-focused residential home phone service. Customers use Ringable-provided analog telephone adapters (the “RingBox”) and standard telephones to place and receive calls within the United States. Ringable’s service is designed for low-volume, person-to-person calling between children, parents, relatives, and other trusted contacts, rather than for high-volume or commercial calling.

Ringable’s core platform uses SIP-based call control and connects to one or more upstream wholesale carriers for access to the public switched telephone network (PSTN). Ringable does not operate its own PSTN-facing switches or interconnection facilities and does not hold its own STIR/SHAKEN Service Provider Code (SPC) token. Ringable is a voice service provider serving end users; it does not function as a gateway provider or a non-gateway intermediate provider.

2. STIR/SHAKEN Implementation Status and Basis for No Implementation

At this time, Ringable has not implemented the STIR/SHAKEN call authentication framework on any portion of its own network. All outbound calls placed by Ringable customers are handed off to upstream wholesale carriers that are listed in the FCC’s Robocall Mitigation Database and that implement STIR/SHAKEN on their own networks where required by the Commission’s rules.

Ringable has certified in the Robocall Mitigation Database as a “Voice Service Provider without a STIR/SHAKEN implementation obligation.” Ringable relies on 47 C.F.R. § 64.6305(d)(2)(i) as the basis for this status because it does not control the network infrastructure or PSTN-facing facilities on which STIR/SHAKEN would be implemented, and therefore does not have a direct STIR/SHAKEN implementation obligation. Instead, Ringable relies on its upstream providers’ STIR/SHAKEN implementations while subjecting all calls it originates to the robocall mitigation measures described below, consistent with 47 C.F.R. § 64.6305(a).

3. Robocall Mitigation Practices (Technical and Procedural)

Ringable employs a multi-layered robocall mitigation program that combines customer vetting (“know your customer”), service design constraints, technical controls, monitoring, and prompt enforcement. These measures are intended to be reasonably expected to prevent the origination of illegal robocalls and to quickly identify and stop any unlawful traffic that might attempt to use Ringable’s service.

3.1 Customer Vetting – “Know Your Customer” (KYC)

Ringable applies a know-your-customer process to all new accounts before enabling service. Key elements include:

- Identity and address collection: Ringable collects the customer’s name, email address, and physical service address for each household line.
- Service address validation: Ringable verifies that the service address is a plausible U.S. residential location and uses the address for 911 routing purposes.
- Payment verification: Service is activated only after a valid payment method has been provided and passes fraud screening through Ringable’s payment processor using Address Verification.
- Service eligibility limits: Ringable markets and provides its service only for residential, family use. The Terms of Service prohibit use of the service for outbound call centers, lead-generation operations, auto-dialed campaigns, or other high-volume or commercial calling activity.
- Ongoing review: Ringable reserves the right to request additional information, temporarily suspend service, or terminate accounts where usage patterns, complaints, or other indicators suggest potential illegal robocall activity or other misuse.

3.2 Service Design Reducing Robocall Risk

Ringable’s service is intentionally designed in ways that make it unattractive for illegal robocallers:

- The product is positioned as a kid- and family-focused home phone solution, not as a high-volume business or telemarketing platform.
- Typical usage consists of low-volume, person-to-person calls between children, parents, and known contacts such as relatives, neighbors, and local community members.
- Parents can configure each line with features such as approved caller lists, time-of-day restrictions, and other controls that further limit calling patterns to those consistent with family use.

3.3 Technical Call Filtering and Controls

Ringable provides technical tools that can be applied on a per-subscriber and network basis to limit or block undesired calling activity:

- Per-line outbound controls: Parents may define an allowlist of telephone numbers that their child is permitted to call. Calls to non-allowed destinations can be blocked or routed to a controlled announcement.
- Per-line inbound controls: Parents may define approved inbound caller lists and explicit blocklists. When filtering is enabled, calls from unapproved or blocked numbers may be rejected or diverted instead of ringing the child's phone.
- Time-of-day and day-of-week blocking ("Quiet Time"): Parents can configure time windows during which inbound and/or outbound calls are not permitted. Calls attempted during blocked windows are rejected or redirected according to Ringable's policies.
- Global and account-level policy controls: Ringable can apply network policies to immediately block known bad destinations, suspicious traffic patterns, or other behavior inconsistent with normal household use.

3.4 Monitoring, Analytics, and Blocking of Suspected Illegal Traffic

Ringable reviews call detail records and uses rule-based monitoring to identify abnormal or potentially unlawful calling behavior. Examples include:

- Unusual spikes in call attempts or concurrent calls from a single line.
- Large numbers of very short calls, especially to many distinct destination numbers.
- Calling patterns inconsistent with a typical child- or family-focused line.

When monitoring or complaints indicate possible illegal or abusive calling, Ringable may temporarily disable outbound calling, restrict calls to an allowlist, block specific numbers, or terminate the account, depending on the severity and circumstances. Ringable also reviews and acts on any complaints received from consumers, upstream carriers, or regulators relating to calls originating from its network.

3.5 Know-Your-Upstream-Provider Program

Ringable maintains a know-your-upstream-provider program. Ringable only uses upstream voice providers that are registered in the FCC's Robocall Mitigation Database and that have represented that they implement STIR/SHAKEN and maintain their own robocall mitigation programs in accordance with FCC rules.

- Ringable confirms that each upstream provider is listed in the Robocall Mitigation Database and monitors for changes to that status.
- Contracts and service agreements require compliance with applicable FCC robocall mitigation requirements, including support for traceback and cooperation with regulators.
- If an upstream provider's compliance status becomes questionable, Ringable will reassess the relationship and, if needed, transition traffic to a provider that remains in good standing.

4. Traceback and Enforcement Procedures

Ringable commits to respond fully and in good faith to traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to do so within 24 hours of receipt

whenever feasible. Ringable will cooperate with these entities to identify the source of suspect calls and to stop any illegal robocall activity using its service.

When a traceback indicates that a call originated from or transited a Ringable customer, Ringable will:

1. Identify the associated subscriber account and relevant call detail records for the time period in question.
2. Provide the requested information to the traceback requester consistent with applicable laws and privacy obligations.
3. Evaluate whether immediate mitigation is required, which may include temporary suspension, restrictions on calling, or account termination.
4. Document the incident and any remedial measures taken for future reference and program improvement.

5. Cooperation and Record Retention

Ringable maintains call detail records for a period sufficient to support traceback requests and internal investigations, currently targeted at not less than twelve (12) months, subject to technical and legal constraints. Ringable will fully cooperate with inquiries from the FCC, law enforcement, and the industry traceback consortium relating to suspected illegal robocalls, including providing call records and other information as appropriate.

Where permitted by law and by contractual obligations, Ringable may also share information about confirmed bad actors with its upstream providers or other trusted industry partners to help prevent future abuse.

6. Certification Statement

I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that Ringable LLC has implemented the measures described above and will continue to maintain and update its robocall mitigation program as necessary to prevent the origination of illegal robocalls on its network.

Signed: _____

Name: Irvine Pascual

Title: Vice President

Date: 12/1/2025