Scamcatch LLC Robocall Mitigation Plan

Effective November 20, 2026

1. The company and the service

Scamcatch LLC (“ScamCatch”), FCC Registration Number 0039134036, provides an AI call screening service to consumers in the United States through the ScamCatch app for iPhone and Android. The service is in a limited beta. ScamCatch files in the Robocall Mitigation Database as a voice service provider.

A call reaches a subscriber through ScamCatch in five steps:

1. The subscriber sets conditional call forwarding on their own mobile line to a dedicated ScamCatch number. Their phone declines or silences callers it does not know, and their mobile carrier forwards those calls to the ScamCatch number.
2. Every ScamCatch number is a Telnyx number. Telnyx answers each call on its own network, at the direction of ScamCatch’s software, and streams the caller’s audio to ScamCatch’s screening system in its cloud back end.
3. The subscriber’s greeting and a notice that the call may be recorded play first. Then ScamCatch’s AI screening system asks the caller why they are calling.
4. A caller judged to be a scam or spam hears a short announcement, and the call ends. A caller who says nothing is disconnected. When the subscriber has shared their contacts with ScamCatch, a saved contact whom they declined goes straight to voicemail.
5. For a caller judged to be a real call, Telnyx connects the same incoming call to the ScamCatch app on the subscriber’s phone over the internet. If the app does not answer, the caller reaches voicemail.

Every ScamCatch call has two parts, and only the first touches the public telephone network:

- **The incoming call.** The caller’s call comes in from the public telephone network. The subscriber’s mobile carrier forwards it to the ScamCatch number, and Telnyx answers it.
- **The connection to the subscriber.** When ScamCatch puts a caller through, it does not place a new phone call. Telnyx connects the same incoming call to the ScamCatch app on the subscriber’s phone over the internet, and the subscriber answers in the app.

ScamCatch never places a call to the public telephone network. It makes no callbacks, no transfers to a phone number and no calls to a subscriber’s mobile number, and its software cannot send a call to a phone number. Subscribers cannot place calls through ScamCatch either: the Call buttons in the app open the phone’s own dialer, and those calls go through the subscriber’s own mobile carrier. ScamCatch does not carry calls for other phone companies or pass calls on to them. Every call it receives ends in screening, in voicemail or in the ScamCatch app.

2. STIR/SHAKEN status

ScamCatch has not implemented STIR/SHAKEN and has no obligation to, because it lacks control of the network infrastructure needed to implement it. Telnyx answers and carries every ScamCatch call on Telnyx’s own network. ScamCatch runs no switch of its own and directs calls only through Telnyx’s call control service. ScamCatch certifies “No STIR/SHAKEN

implementation” on that basis.
Authentication. ScamCatch originates no calls, so it has no calls to authenticate.
Verification. ScamCatch does not check caller ID signatures itself. Telnyx’s Inbound Call Screening is turned on for every ScamCatch number and rejects calls based on caller reputation and STIR/SHAKEN attestation before they reach ScamCatch (section 6). ScamCatch never approves a call because of its caller ID.

3. How the service design prevents illegal robocalls

The most effective step ScamCatch takes is structural. Its service cannot place a call to the public network, so it cannot be used to originate robocalls or to spoof caller ID.

- ScamCatch’s software can connect a call only to the ScamCatch app over the internet, never to a telephone number.
- Subscribers cannot place calls through ScamCatch, so no subscriber can send traffic into ScamCatch’s service.
- ScamCatch numbers are not published. A person who dials one directly is screened in the same way as a forwarded caller.

The service also exists to protect consumers from unwanted and fraudulent calls. Saved contacts the subscriber has shared with ScamCatch are never screened. Every other caller that reaches ScamCatch is screened, and callers judged to be scams or spam are disconnected (section 6).

4. Know your customer: new and renewing subscribers

ScamCatch meets 47 CFR 64.1200(n)(4) with the following steps. They apply at sign-up and for as long as an account exists:

- Each subscriber signs in with Apple, with Google, or with an email address confirmed by a link.
- Each subscriber proves control of their own US mobile number by entering a one-time code sent to it by text message. ScamCatch’s server confirms the code with the text service and keeps only the number the code was sent to. The mobile number cannot be a ScamCatch number.
- A ScamCatch number is assigned only after the mobile number is verified, the subscriber’s greeting is approved and the subscriber’s phone is registered. Each account has one ScamCatch number.
- A ScamCatch number is never reassigned to a different subscriber. After an account is deleted, its number is held only for the same verified mobile number and is later released back to Telnyx.
- Accounts are never merged. A new login, such as a sign-in on a new phone, is linked to an existing account only after the account’s current app key or a new mobile verification proves ownership.

Because subscribers cannot place calls through ScamCatch, the risk this rule addresses, a customer using the network to originate illegal calls, does not arise. Renewal does not change any of these controls.

5. Upstream provider

ScamCatch receives calls from one upstream provider, Telnyx, LLC, which supplies its numbers and answers and carries its calls. ScamCatch accepts calls from no other provider.
Telnyx, LLC (FRN 0018998724) is listed in the Robocall Mitigation Database; ScamCatch confirmed the listing on November 20, 2026. ScamCatch will check the listing again each year when it recertifies this filing, and will stop accepting calls from any provider that is removed from the Database.
ScamCatch has no downstream providers. It never sends a call on to another phone company, and approved calls go only to its own app over the internet.

6. Call analytics

ScamCatch judges every call before it reaches the subscriber:

- Telnyx's Inbound Call Screening, turned on for every ScamCatch number, rejects calls based on caller reputation and STIR/SHAKEN attestation before they reach ScamCatch.
- ScamCatch's own screening system judges every other call. The caller first hears the subscriber's greeting and the recording notice. An AI voice built on Google's Gemini Live then asks the caller short questions about why they are calling. It is instructed never to give out information or agree to anything for the subscriber.
- Jev, a service from TypeSafe, scores the caller's words against yes-or-no questions about scams, spam and real calls, and ScamCatch's code makes the decision. The questions are ScamCatch's own built-in set, plus any rules the subscriber adds about whom to put through or block.
- A scam or spam decision ends the call after a short announcement, and the caller cannot leave a voicemail. A caller who says nothing is disconnected. If screening reaches its limit without a clear answer, the call goes the way the screening leaned most: put through, or ended as a scam or spam. If a call cannot be judged at all, for example because a screening service fails, the call ends.
- A call is never approved because of its caller ID or a match with the subscriber's contacts.

ScamCatch's outside vendors in call analytics are Telnyx, for Inbound Call Screening; Google, for the AI conversation; and TypeSafe, for Jev.

7. Traceback and cooperation

ScamCatch commits to respond fully and within 24 hours to traceback requests from the Commission, civil and criminal law enforcement agencies and the industry traceback consortium, and to cooperate with them in investigating and stopping any illegal robocaller that uses its service. If the Commission's Enforcement Bureau notifies ScamCatch of suspected illegal traffic, ScamCatch will investigate promptly and take the steps the notice requires.
For each call that hears ScamCatch's full greeting and recording notice, or stays on through the voicemail prompt to the beep, ScamCatch keeps a record of the calling number (or "private"), the subscriber account it was for, the time of each step and the screening outcome. These are kept until the subscriber deletes the account. Because every call reaches ScamCatch from Telnyx, ScamCatch can name its upstream provider for any call it handled. Requests may be sent to the robocall mitigation contact in section 9.

8. Enforcement history

In the past two years, neither ScamCatch nor any of its affiliates or principals has been the subject of a formal Commission, law enforcement or regulatory action or investigation involving suspected unlawful robocalling or spoofing, or a deficient Database certification or mitigation plan.

9. Robocall mitigation contact

Daniel Baek, Chief Operating Officer, Compliance
22914 Colombard Ln, Unit 5, Diamond Bar, California 91765
(909) 367-1583 · Daniel.Baek@scamcatchai.com

10. Review and updates

ScamCatch will update this plan and its Database filing within 10 business days of any change to the information in them, and will recertify its filing each year by March 1. ScamCatch is building its own call system, in which its own switch will answer calls on numbers from another carrier. Before that system serves any subscriber, ScamCatch will update this plan, its upstream provider and its STIR/SHAKEN status. ScamCatch will not add any way for subscribers to place calls, or any call from its service to the public network, without first revising this plan and its STIR/SHAKEN status.
Daniel Baek, Chief Operating Officer, Scamcatch LLC
November 20, 2026