

LEARNLY VENTURES INC. ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like Learnly Ventures INC. (“Learnly”), to, among other things, file certifications and robocall mitigation plans in the FCC’s Robocall Mitigation Database (“RMD”). 47 CFR § 64.6305; see also *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023) (“Sixth Caller ID Authentication Report and Order”).

The FCC requires that all voice service providers certify in the Commission’s RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that it originates, carries or processes are subject to a robocall mitigation program consistent with the Commission’s rules.¹ The provider’s mitigation plan “shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond 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 its service to originate calls.” 47 C.F.R. § 64.6305(a)(2). The Commission has explained that such a program is “sufficient if it includes detailed practices that can reasonably be expected to significantly reduce” the provider’s origination of illegal robocalls, and the provider complies with the practices described in its plan. *Sixth Caller ID Authentication Report and Order* ¶ 31.

Learnly provides a hosted outbound calling and customer relationship management platform to licensed insurance agencies in the United States. It resells interconnected VoIP service obtained on a wholesale basis from an underlying carrier and is the retail provider of record to its customers, which are business end users. Learnly does not serve other carriers, does not act as a wholesale originator, accepts no traffic from foreign providers, and is not an intermediate provider. Its customers are United States insurance agencies; foreign use of the platform is not permitted, and no foreign provider or end user originates traffic through it.

Congress addressed two categories of unlawful call in the TRACED Act’s definition of a robocall violation: 47 U.S.C. § 227(b) and § 227(e).² Learnly notes that, by design, its platform is provisioned so as to substantially curtail its end users’ opportunity to place either category of call.

First, the platform cannot generate telephone numbers. Every number dialed originates in a lead record the customer supplied by import or through its own integrations; the system has no random or sequential number generator and no capacity to produce one. Under *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021), a system without that capacity is not an automatic telephone dialing system, so § 227(b) liability premised on autodialer use should not arise from the

platform's own capabilities.

Second, calls originated through the platform are placed by live agents. Learnly does not offer prerecorded or artificial-voice messaging to its customers: no customer has a voicemail message configured for delivery, and the platform refuses any such delivery where no active message resolves. The platform accordingly originates no calls delivering a prerecorded or artificial voice.

Third, Learnly's end users can present outbound caller identification only from numbers recorded in the platform's own inventory and associated with their account. Arbitrary or free-form caller identification cannot be entered at dial time. Section IV describes how numbers enter that inventory. Given those caller identification practices, Learnly's customers should be incapable of a spoofing violation prohibited by 47 U.S.C. § 227(e).

Learnly will update this description and its certification if any of those three constraints changes. This document outlines Learnly's robocall mitigation plan.

¹ See <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf> (WCB Jan. 25, 2024 Public Notice).

² The TRACED Act defines a "robocall violation" as "a violation of subsection (b) or (e) of section 227 of the Communications Act of 1934." TRACED Act § 11(d), Pub. L. No. 116-105, 133 Stat. 3274 (2019). The Commission's codified rules do not themselves define "robocall," so Learnly focuses, as it must, on the two categories of unlawful call that Congress expressly addressed.

II. Learnly's Know Your Customer ("KYC") Standards

Learnly focuses its business and operations on the licensed insurance agency segment of the market. It does not offer self-service, anonymous, or trial access. Every customer is onboarded under a formal written agreement, and no account can originate calls until it is affirmatively activated: a new agency record is created in a pending state and must be transitioned before any dialing capability exists.

Learnly's customer identification extends below the entity to the individual placing the call, which is a direct consequence of the regulated market it serves:

- **Every caller is licence-verified against a state authority.** Each individual who places calls must submit producer licence details, including National Producer Number, licence number and state of licensure. The submission remains pending until reviewed and approved by an authorised administrator, and an individual whose licence has not been approved cannot reach the dialing application at all.
- **Dialing permission is granted per person, not per account.** A newly added user is inactive on every campaign by default and must be individually approved before placing a call.
- **Dialing permission is revocable per person.** Learnly can withdraw one individual's dialing permission without suspending the agency.

III. Learnly's Acceptable Use Policy

As part of its customer-onboarding process, Learnly's customers contractually agree to terms that track the governing statutes. Among other things, a customer will not use the services to:

- place calls to numbers on any do-not-call list absent a valid, documented exemption;
- engage in spoofing, "snowshoeing," or number rotation to evade blocking or labeling, or transmit inaccurate or misleading caller identification;
- place calls that are abusive, threatening, harassing, deceptive or fraudulent, or that impersonate a government agency, carrier, financial institution or any other person;
- deliver prerecorded or artificial-voice messages without required consent; or
- rely on consent obtained through consent stacking, pre-checked boxes, dark patterns, or forms that do not clearly and conspicuously identify the seller and the purpose.

The agreement further requires each customer to obtain and maintain **its own Subscription Account Number** for the National Do Not Call Registry and any required state registry subscriptions, and not to use another person's Subscription Account Number; to scrub its calling lists against the National Registry, applicable state registries and its own internal do-not-call list at the intervals required by law, and no less frequently than every 31 days for the National Registry; to maintain an internal do-not-call list and a written do-not-call policy; to train its agents; and to honour every do-not-call request immediately and permanently. A separate provision requires that every lead, list or live transfer used with the services was lawfully obtained and is supported by valid, unexpired, properly scoped consent, with the consent record retained.

Learnly's contracts with its customers stipulate that Learnly is authorized to suspend and/or terminate all services in the event of a violation, and entitle Learnly to audit a customer's Subscription Account Number, do-not-call policy, consent records for sampled leads and agent licensing information.

IV. Telephone Number Authorization and STIR/SHAKEN Capabilities

Learnly holds no Operating Company Number and no Service Provider Code token issued by the STI-Policy Administrator. It does not sign calls with its own certificate and has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

Learnly is a non-facilities-based reseller without direct access to numbering resources. Under the STI-Policy Administrator's token access policy, a service provider must hold an Operating Company Number in order to be issued a Service Provider Code token. Holding none, Learnly is at present incapable of obtaining the certificate necessary to participate in the framework, and is therefore within the extension provided by 47 C.F.R. § 64.6304(b), which applies until such time as a provider becomes capable of obtaining such a certificate. Learnly does not treat this as a permanent position: it has registered with the Universal Service Administrative Company, is filing in this Database concurrently, and is pursuing an Operating Company Number. Learnly will

amend this certification when it becomes capable of obtaining a token.

The majority of telephone numbers in service are acquired by Learnly directly from its underlying carrier and assigned to a customer, so the right to use them is established at the point of purchase and recorded against that customer. Where a customer presents a number obtained elsewhere, Learnly's customer agreement requires it to warrant that it is the subscriber of record or holds written authorization from the subscriber of record, and to supply letters of authorization, invoices or other proof in the form Learnly requests before and during use. Learnly states the present limit of that practice plainly: the authorization is required by contract and produced on request, and is not today a precondition enforced by the platform before a customer-supplied number is used. Learnly is implementing that precondition, and notes that an unverified number cannot in any event be signed at full attestation by an upstream carrier, so its interest in closing this gap is both regulatory and operational.

V. Call Origination Controls

Every call originated on the platform passes through one compliance evaluation component. There is no alternate path: preview dialing, manual dialing, scheduled callbacks, automated dialing and calls initiated through Learnly's API all route through the same evaluation. It operates fail-closed — if the evaluation cannot complete, or the corresponding audit record cannot be written to durable storage, the call is blocked rather than allowed. Automated tests fail Learnly's build if a code change introduces a dialing path that bypasses it.

Four controls within that component cannot be disabled by any customer or campaign setting:

- **Internal do-not-call screening.** Learnly maintains a per-customer internal list. Every opt-out captured on a call is written to it permanently by two independent paths — a post-call disposition rule applied when the call is logged, and a direct consent-revocation function. A number on the list is blocked from all subsequent dialing by that customer.
- **Telephone number validity** is checked before dialing.
- **Lead retirement by age** removes stale contact data from the dialable pool.
- **The audit record** described in Section VIII is written for every evaluation.

Two further controls are configured per campaign and are enforced by default. The first is the permitted calling window, evaluated against the called party's location at the time of the call. A federal baseline of 8:00 a.m. to 9:00 p.m. called-party local time applies to every call, and the evaluation is fail-closed: where a reliable time zone cannot be determined for the called number, the call is blocked rather than placed. A configured set of states carries restrictions stricter than that baseline, including narrower hours, Sunday restrictions and named-date holiday blocks. Learnly notes the limit of that table candidly: it is a representative encoding of stricter-than-federal restrictions rather than an exhaustive fifty-state compilation, holiday blocking is applied to the subset of states configured for it rather than nationally, and state-of-emergency calling bans, which require a live data feed, are out of scope. The customer agreement places

responsibility for configuring and complying with calling-hour, holiday and frequency restrictions in every jurisdiction the customer calls on the customer.

The second is a licensure restriction: a lead in a given state may be dialed only by an agent licensed in that state, evaluated at the time of the call against the dialing agent's verified licences.

VI. Monitoring and Analytics

The Commission's rules provide that a provider's plan should describe the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s). 47 C.F.R. § 64.6305(d)(1)(ii). The Commission has acknowledged that it does "not specifically require providers to use call analytics." *Sixth Caller ID Authentication Report and Order* ¶ 40 & n.156. Learnly's monitoring is directed at the reputation and labeling status of the numbers it assigns:

- **Carrier analytics engine lookups.** Learnly queries the analytics engines that terminating carriers rely on — **TNS, Hiya and First Orion** — resolving each carrier to its governing engine, and separately queries **Nomorobo** as a carrier-independent authority.
- **Handset-level health checks.** A number health check submits an assigned number to a vendor that reports spam-label status across a grid of carriers and devices, returning per-carrier verdicts and screenshots of what a handset actually displays.
- **Per-number reputation history** is retained against each number, so a degrading number is visible over time rather than only at the moment of complaint.

Learnly states the limit of this candidly: these systems observe how the network treats Learnly's numbers. They are not outbound traffic-pattern analytics, and Learnly does not presently operate short-duration, answer-seizure-ratio or ANI-cardinality analysis, nor a third-party origination mitigation product. Learnly acts on reputation degradation observed on an assigned number, treating it as a signal warranting review of the customer holding that number.

VII. Division of Responsibility

Learnly provides software that its customers operate. It does not select the parties its customers call, the timing of those calls, the number presented, the script used, or whether a call is recorded. Each customer is an identified, contracted, state-licensed insurance agency that makes those decisions itself, and the customer agreement states that allocation expressly.

Registry scrubbing is performed by the customer under the provisions described in Section III, as the party holding lead provenance and consent evidence; Learnly does not duplicate it at the platform layer. Relatedly, when leads are imported Learnly deliberately does not write consent records or scrub-clean markers on the customer's behalf. It cannot verify either, and a synthetic record would represent to Learnly's own controls that a lead carries a lawful basis it may not have. That constraint is enforced in the import path itself.

These allocations do not displace Learnly's own controls, which operate independently and cannot be switched off by a customer: the fail-closed evaluation point and non-disableable screening described in Section V, the number authorization practices in Section IV, the monitoring in Section VI, and the audit record in Section VIII.

VIII. Commitment to Timely Traceback Responses and Cooperation

Learnly 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 its service to originate calls. Learnly will dedicate sufficient resources to provide timely and complete responses to such requests, and will investigate suspicious activity found by its monitoring systems or reported to it by appropriate parties and take appropriate action.

Learnly can meet that commitment because it records every origination decision. One audit record is written per evaluation, capturing the number called, the originating customer, the individual user, the campaign and the outcome. Numbers are recorded against the customer holding them. Any number and time can therefore be resolved to a specific identified customer and a specific licensed individual. Call recordings and transcripts are retained for ninety days and call detail records for eighteen months, which exceeds the window in which tracebacks are ordinarily raised. The customer agreement separately requires each customer to retain its own compliance records, including consent and do-not-call records, for five years after the relevant call, and to produce consent records, scrubbing records and calling-window logs to Learnly within five business days of request.

A traceback, regulatory inquiry or consumer complaint is reviewed by Learnly's robocall mitigation contact on receipt. Learnly resolves the number and time to the originating customer and the individual user from its audit records, and requests that customer's consent records, scrubbing records and calling-window logs. Where those records do not substantiate a lawful basis for the calls, or the customer fails to produce them, Learnly withdraws the individual's dialing permission or suspends the agency. Suspension is effective across the platform rather than at a single surface: a suspended agency's dialing stops, its automated workflows cease, its machine credentials are refused, its outstanding invitations are revoked and its users' sessions are terminated. Repeat or unremedied findings result in termination.

Learnly reviews this program annually and upon any material change to the practices described, and will update this description and its Database filing accordingly.