

A copy of this letter was sent via overnight mail on 2024-12-30 to: Federal Communications Commission 45 L Street NE, Washington, DC 20554

A PDF copy was also be uploaded to the RoboCall Mitigation Database and a copy was also emailed in pdf format will be uploaded to rmd-compliance@fcc.gov

Robocall Mitigation Plan for SymplyFi (RMD0005319)

This robocall mitigation plan is for SymplyFi, with headquarters at 2099 Monroe Drive Ste 777 Atlanta GA 30324.

We perform the following roles in the call chain:

A voice service provider with a STIR/SHAKEN implementation obligation serving end-users.

SymplyFi has not been prohibited from filing a certification in the Robocall Mitigation Database.

SymplyFi does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

SymplyFi uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

SymplyFi provides services directly to end-users with physical retail stores and business locations.

We verify the business entity, business activity & physical location of every customer before activation.

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with each customer.

Our contractual provisions with customers prohibit them from initiating illegal robocalls.

If we find a customer initiating illegal robocalls they are warned to stop and we terminate their service if they continue.

Know Your Upstream Provider

We use upstream Tier 1 carriers and only originate or terminate calls with Tier 1 carriers each of whom have their own robocall mitigation strategies.

We verify that our upstream providers have a certification in the Robocall Mitigation Database prior to using their services.

Robocall Mitigation Program

We only provide outbound calling for contracted customers (end-users) on our system.

All outbound calls are required to use calling numbers configured and owned by the specific customers.

We immediately investigate any identified suspicious outbound calls to determine if the customer was attempting to make illegal robocalls.

If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic.

If they continue to send traffic that appears to be unlawful, then we terminate their service.