

Fastcall411, Inc ("Fastcall") Robocall Mitigation Policy  
March 29, 2024

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. The Robocall Mitigation Plan is written to ensure that illegal traffic does not originate on the company's voice applications.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that details the reasonable steps taken to avoid originating illegal robocalls, demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls. The plan is filed in the Robocall Mitigation Database.

This mitigation plan is submitted by Fastcall, a softphone phone application installed in Salesforce. Fastcall is a small, niche voice service provider with less than 100 business clients. Outbound customer service phone calls can be made from the Salesforce CRM (customer relationship management). Inbound calls are received by provisioned phones. Fastcall in turn uses Twilio and other CPaaS providers for phone services. Fastcall has a very strong "know your customer" policy. Customers are enterprise subscribers of Salesforce. Fastcall customers install Fastcall in their Salesforce instance. Fastcall does not sell to unknown customers or consumers. Registration with a valid Employee Identification Number (EIN) is required to use Fastcall services.

Fastcall is partnering with a trusted provider - Twilio - to implement STIR/SHAKEN on behalf of its business customers.

#### General Prohibition Against Illegal Robocalling

Fastcall end-user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service ("TOS") requirements and acceptable use policy ("AUP"). Its existing TOS and AUP prohibit activities generally associated with Robocalling, including, but not limited to:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law; using the Fastcall service to engage in or in connection with fraudulent activities

The company TOS and AUP expressly reference the prohibition on robocalling, and all current subscribers will receive notice of the publication of its updated TOS and AUP. Fastcall end users are notified that the company may take action up to suspension or termination of service for violation of the TOS.

Fastcall utilizes the mitigation technique of "Know Your Customer." Fastcall is a small long-established, niche provider that maintains a close relationship with its subscribers. Its

customers are generally “enterprise” users calling other businesses (B2B.) The customer base does not generate high-volume traffic associated with robocalling, allowing Fastcall to use targeted in-house analytics to potentially identify, monitor, alert, and apprehend suspected robocalling activities. Fastcall has set a call level based on the customer size. The “large volume calling capability” level is subject to change. Fastcall has a screening for new customers requesting service:

- Businesses must provide a tax ID and verification as to the nature of the business
- The Fastcall service is automatically suspended if the volume of calls exceeds a set limit
- Fastcall serves a small number of known businesses who accept Fastcall’s policies and efforts to prevent the Fastcall service from being used for illegal robocalling.

Fastcall has developed custom in-house software that allows for real-time traffic monitoring and flags call patterns indicative of potential illegal robocalling. The software is being enhanced to automatically disable any subscribers associated with flagged call patterns.

Fastcall will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. Fastcall will dedicate sufficient resources to provide prompt and complete responses to traceback requests.