

Robocall Mitigation Plan

Progressive Computer Research, Inc. (“PCR”) resells service using Underlying Carriers (“Partners”), and relies on their commitment and processes to combat Robocalls. Our Partners provide DIDs directly to our SIP PBX customers.

PCR commits, by contract with its Partners, that all users of its services comply with applicable laws prohibiting illegal robocalling and providing for blocking and/or termination of services for those that breach such provisions.

PCR’s Robocall Mitigation Plan is premised upon a set of technical and operational procedures, the details of which can be summarized as follows:

- 1) **Prevention:** PCR has a stringent on-boarding screening process designed to prevent those that may engage in illegal robocalling from becoming customers at the outset. PCR uses a direct sales model and verifies the business activity, physical location, and credit worthiness of every customer. After our initial “Know Your Customer” screening and customers are on-boarded, PCR works to stay closely aligned with its customers regarding the industry’s anti-robocalling objectives. PCR screens all applicants for its services to determine if they are intending to use such services for autodialing from a database of numbers for purposes of telemarketing without having received written permission from the called parties. Calls to wireline (landline) numbers for purposes of political campaigning, market research or polling are deemed legal. All of our customers have access to call screening and the ability to block callers by CallerID information.
- 2) **Detection:** PCR monitors call volume to detect and analyze the use of its services and traffic that helps to determine when illegal and inappropriate robocalling activity may be occurring. When unlawful robocall campaigns are detected, PCR works to stop the unlawful activity as quickly as possible. PCR also relies on its Partners commitment to continuously monitor calling patterns in and out of network to identify fraudulent traffic, including robocalling, traffic pumping, and international toll fraud. PCR will block services to a customer if it determines that the customer is using the services for any illegal activities, including robocalling. Such customer’s agreement will be terminated if the violation is determined to be intentional. We log calling activity to flag calling patterns that are indicative of robocalls, including both toll fraud and calling patterns such as automatic dialers.
- 3) **Mitigation:** Our customers have a rate limit and internal alarms are triggered if a customer’s concurrent call limit is reached. In order to prevent the delivery of unwanted and illegal traffic to the greatest degree possible, PCR utilizes all STIR/SHAKEN features provided by our partners as well as call blocking tools that are designed to block calls from invalid and illegal telephone numbers in keeping with industry best practices and the FCC’s recommendations. PCR has contracted with its voice provider Partners to attest, at the applicable levels, its customers’ traffic originated on PCR’s network.

Traceback: PCR commits to respond to all traceback requests from the Federal Communications Commission, law enforcement and the industry traceback consortium and to cooperate with such entities, and its Partners, in investigating and stopping any illegal robocallers from using its services to originate calls, and that all voice traffic that originates on its network is subject to this robocall mitigation program.