



Private National Mortgage Acceptance Company, LLC Robocall Mitigation Strategy

1. Introduction

Private National Mortgage Acceptance Company, LLC (PennyMac), a financial institution, is committed to complying with all applicable federal regulations, including those aimed at mitigating illegal robocalls. As a financial institution, we understand the importance of maintaining the trust and security of our customers' communications. To that end, we utilize Public Switched Telephone Network (PSTN) carriers for our voice traffic. These carriers have implemented robust robocall mitigation strategies, including STIR/SHAKEN technology, to ensure the integrity of our network. This document outlines PennyMac's comprehensive Robocall Mitigation Strategy, detailing the specific steps taken to prevent the origination, transmission, and termination of illegal robocalls.

2. Robocall Mitigation Strategy

PennyMac has implemented a robust robocall mitigation program that addresses both inbound and outbound calls. This program includes the following key elements:

- **New and Existing Customer Verification:** PennyMac verifies the business activity and creditworthiness of every customer before establishing a business relationship. This helps to prevent fraudulent activity and ensures that our services are not used for illegal robocalling purposes.
- **Call Analytics:** PennyMac leverages call analytics dashboards provided by our PSTN carriers to monitor call traffic in real-time. These dashboards provide visualizations and reports on call volume, duration, and other key metrics. Our team, as well as our PSTN carriers, regularly analyzes this data to identify any irregular activity, such as sudden spikes in call volume or calls from suspicious sources. Any anomalies are investigated to determine the source and nature of the activity, and appropriate action is taken to mitigate potential threats.
- **Carrier Partnerships:** PennyMac partners with a select group of trusted PSTN carriers to originate and terminate our voice traffic. These carriers are chosen based on their strong commitment to robocall mitigation and adherence to industry best practices, including full implementation of STIR/SHAKEN call authentication technology.

Our current partners include:

- Bandwidth.com CLEC, LLC (FRN: 0017042060)
- 382 Communications Corporation (FRN: 0020540308)
- Broadband Dynamics, L.L.C. (FRN: 0006833412)

Each of these carriers is certified in the Robocall Mitigation Database (RMD), demonstrating their compliance with FCC regulations and providing readily accessible

contact information for robocall mitigation-related inquiries. We maintain close communication with our carrier partners to ensure ongoing adherence to evolving robocall mitigation standards.

- **STIR/SHAKEN Implementation:** PennyMac leverages the STIR/SHAKEN framework through our partnerships with multiple PSTN carriers who have fully implemented STIR/SHAKEN. We rely on this implementation to fulfill the requirements of the framework and actively monitor our carriers' compliance with STIR/SHAKEN standards.
- **Upstream Provider Monitoring:** PennyMac maintains close partnerships with all our upstream providers, formalized through contracts that outline our shared commitment to network security and compliance with industry best practices. We are intimately familiar with their services and regularly communicate with them to ensure adherence to evolving FCC regulations.
- **Gateway-Level Blocking:** Our network infrastructure includes robust call blocking capabilities at the gateway level. This prevents unsolicited and illegal robocalls from reaching PennyMac employees and customers.
- **TCPA Compliance:** All outbound calls initiated by PennyMac are conducted in full compliance with the Telephone Consumer Protection Act (TCPA) regulations. This includes obtaining proper consent, honoring do-not-call requests, and providing clear identification of the caller.
- **Traceback Cooperation:** PennyMac is committed to fully cooperating with all traceback requests from the FCC and other law enforcement agencies. We have established procedures to ensure that all traceback requests are responded to in accordance with FCC requirements.