

Robocall Mitigation Plan

Overview Our organization is committed to combating illegal robocalls and ensuring compliance with regulatory requirements. This Robocall Mitigation Plan outlines our approach to ensure that all calls made through our systems are legitimate, consented, and compliant with applicable laws and industry standards.

Scope This plan applies to all calls made by our organization to users regarding information on their accounts. All calls will be directed to individuals who have explicitly provided their consent to be contacted.

1. Know Your Customer (KYC) To prevent misuse of our communication systems and ensure compliance:

- **Verification of Customer Consent:** Prior to initiating any calls, we verify that the intended recipient has explicitly consented to receive communications regarding their account. Consent is obtained during account registration or through other documented interactions.
- **Customer Information Accuracy:** We maintain accurate and up-to-date customer information to ensure that calls are directed to the correct individuals.
- **Data Privacy and Security:** All customer data is handled securely and in compliance with data protection regulations, such as GDPR and CCPA.

2. Know Your Upstream Providers We collaborate with trusted upstream providers to ensure secure and compliant call routing:

- **Twilio:** We use Twilio's robust platform for call initiation and management. Twilio's compliance with STIR/SHAKEN protocols and its commitment to combating robocalls align with our mitigation objectives.
- **DIDWW:** DIDWW serves as a reliable provider for phone number services, ensuring seamless connectivity and compliance with regulatory standards.
- **Monitoring and Communication:** Regular communication with Twilio and DIDWW ensures alignment on regulatory updates, best practices, and any required improvements to call handling systems.

3. Robocall Mitigation Measures

- **Consent Verification:** Calls are made only to users who have provided clear consent. Our system maintains a record of consent for audit purposes.
- **Call Authentication:** We utilize STIR/SHAKEN protocols through our upstream providers to authenticate calls and prevent spoofing.
- **Call Monitoring:** Regular audits of call logs are conducted to identify and address any anomalies or unauthorized usage.
- **Training and Awareness:** Employees involved in account-related calls are trained on robocall mitigation practices, legal requirements, and data protection protocols.

4. Regulatory Compliance Our practices are aligned with the Federal Communications Commission (FCC) requirements and other relevant regulatory bodies. We monitor changes in regulations to ensure ongoing compliance.

5. Incident Response In the event of suspected unauthorized or illegal call activity:

- **Investigation:** A thorough investigation is conducted to identify the source and cause of the issue.
- **Mitigation:** Immediate actions are taken to stop unauthorized calls, including working with upstream providers and implementing technical fixes.
- **Reporting:** Incidents are reported to the relevant authorities, as required by law.

6. Continuous Improvement We are committed to regularly reviewing and updating this Robocall Mitigation Plan to incorporate new technologies, industry best practices, and regulatory updates.



Sign