

Robocall Mitigation Program Description

1. Introduction

Stour Marine Ltd. is committed to preventing the transmission of illegal robocalls and fraudulent or spoofed calls over its network. This Robocall Mitigation Program describes the policies, procedures, and technologies we have implemented to meet regulatory requirements set by Ofcom in the UK, as well as the US FCC's regulations under the TRACED Act, ensuring that illegal robocalls are actively monitored, managed, and blocked.

This document outlines our approach to robocall mitigation in the absence of STIR/SHAKEN authentication. We employ a robust combination of caller identification validation, traffic monitoring, and call blocking procedures to prevent the origination and termination of fraudulent and illegal calls on our network.

2. Program Objectives

The objectives of the Stour Marine Robocall Mitigation Program are to:

- Comply with Ofcom's requirements under General Conditions and CLI Guidance, ensuring valid, authorized, and formatted CLI data.
- Fulfil FCC requirements for robocall mitigation, contributing to the FCC's Robocall Mitigation Database as required under 47 CFR § 64.6305.
- Reduce the incidence of illegal robocalls and protect end-users from fraudulent or spoofed call activities.
- Enhance the overall integrity and security of voice traffic on our network.

3. Robocall Mitigation Policies

3.1 Call Validation and CLI Management

- **Valid and Authorized CLI:** Stour Marine ensures that all Calling Line Identification (CLI) data presented on our network complies with Ofcom's CLI Guidance. Only authorized, valid, and correctly formatted numbers are used, and we block calls that fail CLI validation checks.
- **Monitoring of Non-Dialable or Spoofed Numbers:** Our system actively monitors and blocks non-dialable numbers and known high-risk numbers (e.g., those on Do Not Originate lists or other blocklists).

3.2 Customer Screening and Authorization

- **Know Your Customer (KYC) and Due Diligence:** Before onboarding new customers, Stour Marine conducts thorough KYC and due diligence to ensure that numbers are assigned only to legitimate, authorized users, reducing the risk of misuse.

- **Confirmation of Number Use Authorization:** Customers must confirm authorization to use numbers as CLI, especially for high-risk numbers like international or non-geographic numbers.

3.3 Ongoing Monitoring of Call Traffic

- **Real-Time Traffic Analysis:** Stour Marine uses automated systems to monitor call traffic in real time, detecting patterns indicative of robocall or spoofing activities. Indicators include high call volumes, short call durations, and irregular call intervals.
- **Anomaly Detection for Fraudulent Traffic:** The system flags unusual traffic patterns (e.g., high call failure rates, repeated short-duration calls) that are commonly associated with robocalls. Alerts are generated for manual review if abnormal patterns are detected.

4. Robocall Detection and Mitigation Processes

4.1 Robocall Detection

- **Pattern Recognition Technology:** We employ pattern recognition technology to identify suspicious behaviour. This includes monitoring high-volume call origination with low connection rates and other known indicators of illegal robocall campaigns.
- **Call Analytics and Blacklists:** Stour Marine maintains and updates blacklists of known fraudulent numbers and blocklists shared by regulatory agencies or trusted industry partners. Calls originating from these numbers are automatically blocked.

4.2 Robocall Mitigation

- **Blocking of Known Fraudulent Numbers:** Calls from numbers on the DNO list, non-dialable numbers, and known spam sources are blocked at the network level.
- **Automated Call Blocking Thresholds:** We apply thresholds for call volumes and call failure rates, dynamically blocking calls that exceed established safe limits. Calls flagged as high-risk are blocked and logged for further analysis.

4.3 Response to Robocall Incidents

- **Incident Reporting and Investigation:** Any detected robocall activity is flagged for immediate review. Our Compliance Team investigates the source of the suspicious calls, validates customer use, and takes corrective action if needed, including suspending services.
- **Customer Notification and Remediation:** Customers responsible for originating suspicious traffic are notified and may be required to implement corrective actions, such as additional caller verification processes or traffic control measures.

5. Robocall Mitigation Program Enforcement

5.1 Compliance with Regulatory Authorities

- **Reporting to Ofcom and the FCC:** Stour Marine provides updates to Ofcom on our fraud mitigation measures. For FCC compliance, we submit required documentation to the FCC's Robocall Mitigation Database, certifying that we have implemented a robocall mitigation program.
- **Internal Audits and Reporting:** We conduct yearly internal audits to assess our program's effectiveness, including reviewing blocked call reports, monitoring traffic analysis results, and updating mitigation practices as needed.

5.2 Termination and Blocking of Non-Compliant Customers

- **Customer Contractual Compliance:** Stour Marine's contracts with customers contain strict clauses on CLI and call origination compliance. Non-compliance with CLI and robocall mitigation requirements can result in service suspension or termination.
- **Immediate Blocking of Malicious Traffic:** Any customers found to be originating malicious or illegal robocalls are immediately blocked from the network, and their accounts are flagged for potential termination based on the severity of non-compliance.

6. Program Oversight and Continuous Improvement

6.1 Dedicated Compliance and Security Teams

- **Compliance Officer:** The Compliance Officer oversees robocall mitigation, ensuring that all policies and procedures comply with regulatory standards and are effectively implemented.
- **Security Team:** The Security Team supports real-time traffic monitoring, fraud detection, and incident investigation.

6.2 Training and Awareness

- **Staff Training:** All relevant staff members are trained on robocall detection and mitigation procedures, including recognizing call patterns that indicate potential robocall activities and the steps required to mitigate them.
- **Customer Education:** Stour Marine provides resources to customers on best practices for managing CLI and preventing robocalls, including guidance on caller ID verification and effective number use practices.

6.3 Program Evaluation and Continuous Improvement

- **Annual Review of Program Effectiveness:** We conduct an annual review of the Robocall Mitigation Program to evaluate effectiveness, identify areas for improvement, and adapt to emerging robocall strategies and regulatory updates.

- **Technology Upgrades and Partnerships:** Stour Marine actively explores partnerships with third-party vendors for advanced robocall detection technologies, including analytics and machine learning tools to enhance detection capabilities.

7. Certification with the FCC Robocall Mitigation Database

Stour Marine certifies its compliance with FCC requirements by filing a Robocall Mitigation Certification with the FCC's Robocall Mitigation Database. This certification confirms that:

- Stour Marine has implemented a robust robocall mitigation program, in line with FCC regulations under 47 CFR § 64.6305.
- Our program includes active monitoring, detection, and blocking of suspected illegal robocalls.
- We commit to maintaining compliance with the FCC's robocall mitigation requirements and implementing additional measures if required.

8. Conclusion

Stour Marine's Robocall Mitigation Program is designed to address and mitigate illegal robocalls in compliance with both Ofcom and FCC regulations. Although STIR/SHAKEN is not currently implemented on our network, we maintain rigorous validation, monitoring, and mitigation practices to prevent unauthorized robocalls. This commitment underscores our dedication to maintaining high standards of call integrity, protecting end-users, and supporting global efforts to combat robocall fraud.
