

Heymarket Robocall Mitigation Plan

Last updated: December 19, 2024

Common Sun, Inc. (DBA: Heymarket) is a business text messaging application that enables businesses to manage customer communication through SMS, MMS, and other messaging channels.

Heymarket does not support voice communications services. However, as a texting provider, we have implemented a robust system of checks and safeguards to ensure compliance with industry standards, regulatory requirements, and best practices for protecting consumers from fraudulent or unauthorized communications. Below, we detail our comprehensive approach to preventing misuse.

Know Your Customer (KYC) Process

Our KYC process ensures that every customer or potential customer is thoroughly vetted before they are onboarded. The measures we employ include:

- All potential customers are evaluated for legitimacy and trustworthiness.
- Business customers must provide a legal business name, Employer Identification Number (EIN), physical address, industry type, and business representative contact information.
- Detailed information about the business is collected and reviewed to ensure alignment with our Acceptable Use Policy (AUP).
- Customers must provide opt-in message confirmation, sample messages, terms and conditions, and a clear use case must be submitted and verified.
- All data is validated against regulatory and industry compliance standards.

By employing these measures, we ensure that businesses using Heymarket are legitimate and trustworthy entities.

10DLC Compliance

We are fully compliant with 10DLC (10-Digit Long Code) messaging requirements. Our procedures ensure that all customers meet strict guidelines before their messaging usage can begin.

These include:

1. Business Verification:
 - Customers must submit valid EIN, business details, and registration information.
 - This information is cross-verified with regulatory databases to confirm authenticity.
2. 10DLC Campaign Registration:
 - Each campaign is registered with detailed descriptions of its use case.

- Sample messages are submitted and approved to ensure compliance with regulations.
3. Opt-In Confirmation:
 - Customers must provide proof of recipient consent through opt-in confirmation mechanisms.
 4. Privacy Policy
 - Customers must share their privacy policy that includes opt-in and opt-out language and that they will not sell the contacts that they have to 3rd party services
 5. Terms and Conditions:
 - Customers are required to acknowledge and adhere to our terms and conditions, which strictly prohibit spam, fraud, and any misuse of Heymarket.

Sign-Up Vetting with AI-Powered Trust Scoring

To ensure only reputable businesses gain access to Heymarket, every sign-up undergoes a vetting process using a third-party Artificial Intelligence (“AI”) service. This system evaluates multiple vectors, including:

1. Domain History:
 - We analyze the age, reputation, and activity of the domain associated with the business.
2. Email Address:
 - Validation of email legitimacy, including domain matching and history checks.
3. Location and IP Address:
 - Geographic and IP address validation to ensure alignment with stated business details.
4. Business Size and Type:
 - Evaluation of the business’s scale and industry to confirm its use case aligns with our policies.

The trust score generated by the AI service is a key factor in determining whether the account is approved and if they require further vetting.

Upstream Carrier Relationships

We maintain strong partnerships with our upstream carriers, including Twilio and Bandwidth.com. Our collaborative efforts include:

1. Quarterly Business Reviews:
 - Regular strategic meetings with carriers to discuss compliance updates, industry trends, and partnership goals.
2. Monthly Traffic Reviews:
 - Comprehensive analysis of traffic patterns to identify any anomalies or potential violations.
 - Any suspicious activity is flagged and investigated promptly.

These relationships ensure that our practices remain aligned with carrier requirements and industry best practices.

Acceptable Use Policy (AUP) Checks

Our AUP is a critical safeguard in preventing misuse of Heymarket. To enforce it, we have implemented the following measures:

1. Message Review System:
 - Every message sent via Heymarket is checked against our AUP keywords before being transmitted to the carrier.
 - This ensures no customer violates the terms of use, such as sending spam, fraudulent messages, or other prohibited content.
2. Automated Monitoring:
 - Twilio and Bandwidth.com have algorithms continuously scan outgoing traffic to detect and prevent violations in real-time.

Traffic Metrics and Limits

We employ detailed metrics and limits to control and monitor all messaging traffic. This includes:

1. Outgoing and Incoming Message Tabulation:
 - We track all message sends to ensure compliance with 10DLC campaign limits. We ensure the TPM limits are not exceeded and traffic is restricted or denied from being sent.
2. Custom Limits- List sends:

- Additional limits are set based on our internal policies to prevent overuse or abuse of Heymarket.

Enforcement and Mitigation

Our Terms of Service state that suspected fraudulent, abusive, or illegal activity by our customers may be grounds for termination service, and may be referred to appropriate law enforcement authorities.

Traceback Requests

As noted above, we do not support voice communications services, and as such there is no reasonable basis to believe that we would receive any traceback requests. Nevertheless, we would respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers.