



TRI COMPUTERS

Robocall Mitigation Program Description

Company Name: Junction Computers LTD T/A Tri Computers

Country of Operation: United Kingdom

Date: 19th January 2026

1. Purpose and Scope

Tri Computers is committed to preventing the origination, transit, and termination of unlawful or harmful automated calls, including scam calls, fraudulent traffic, and calls involving spoofed or misleading caller identification.

This Robocall Mitigation Program describes the policies, procedures, and technical controls implemented by Tri Computers to mitigate the risk of illegal or abusive calling activity on its network. The program applies to all voice traffic originated, carried, or terminated by Tri Computers, including traffic from domestic and international customers and interconnecting carriers.

2. STIR/SHAKEN Status

Tri Computers has **not implemented the STIR/SHAKEN caller ID authentication framework**, as STIR/SHAKEN is not currently mandated or required by regulation in the United Kingdom.

While STIR/SHAKEN is a regulatory requirement in certain jurisdictions, such as the United States, it has not been adopted as a compulsory framework by UK regulators. Accordingly, Tri Computers relies on alternative and effective robocall mitigation measures, consistent with UK regulatory expectations and industry best practices, as described below.

3. Robocall Mitigation Measures

In the absence of a STIR/SHAKEN mandate, Tri Computers employs a layered and risk-based approach to mitigate illegal or abusive calling activity, including:

- **Traffic Monitoring and Analysis:** Continuous monitoring of call volumes, calling patterns, call duration, and answer-seizure ratios to identify anomalous or potentially abusive behavior.
- **Customer Due Diligence (Know Your Customer):** Verification of customer identity, business activities, and intended use of voice services prior to onboarding and on an ongoing basis.
- **Upstream and Downstream Provider Due Diligence:** Assessment of interconnecting carriers and service providers to ensure they maintain appropriate controls against fraud and illegal calling.
- **Caller ID Validation:** Screening for invalid, unallocated, or clearly spoofed calling line identification (CLI), with appropriate call blocking or restriction where necessary.
- **Blocking and Filtering:** Blocking or restriction of traffic that is reasonably suspected to be fraudulent, unlawful, or non-compliant with applicable regulations.
- **Rate Limiting and Call Controls:** Application of call rate limits, thresholds, or service suspension where abnormal or suspicious traffic patterns are detected.



TRI COMPUTERS

4. Response to Suspected Illegal Robocall Activity

Where suspected or confirmed illegal robocall activity is identified, Tri Computers takes prompt and proportionate action, which may include:

- Investigation of the relevant traffic and customer account
 - Notification to the customer or interconnected provider
 - Temporary suspension or permanent termination of service
 - Blocking of offending traffic sources
 - Escalation to relevant authorities where appropriate
-

5. Complaint Handling and Industry Cooperation

Tri Computers maintains procedures to receive, review, and respond to complaints related to nuisance calls, scam calls, or suspected illegal robocalling.

The company cooperates with:

- Regulatory authorities
- Law enforcement agencies
- Industry partners and traceback initiatives where applicable

All requests for information or assistance are handled promptly and in good faith.

6. Program Review and Updates

This Robocall Mitigation Program is reviewed periodically and updated as necessary to reflect changes in UK regulations, industry guidance, and emerging risks related to illegal or nuisance calling activity.