WARRANTY SOLUTIONS®
AN AMYNTA COMPANY

Warranty Solutions Administrative Services, Inc.

STATEMENT OF COMPLIANCE WITH FTC SAFEGUARDS RULE

November 15, 2022

Warranty Solutions Administrative Services, Inc. ("Warranty Solutions") has reviewed its policies and procedures regarding the protection of the consumer information we process. We have also reviewed the FTC's "Safeguards Rule" and related comments (the "Rule") to evaluate our compliance with the Rule's requirements. After conducting a comprehensive security audit, Warranty Solutions management has concluded that it complies with the Rule in all material respects.

Warranty Solutions has taken the following steps to confirm that we are complying with the Rule.

1. **Appointment of a "Qualified Employee"**: Glenn Gardner, Chief Information Officer (CIO) is responsible for our information security program.
2. **Completion of Periodic Risk Assessments with Written Report**: Warranty Solutions conducts periodic audits to prepare a risk assessment reported to our management in writing no less than annually to evaluate and assist us in addressing any security risks when we become aware of a need and implements changes as needed.
3. **Design and Implement Safeguards to Control Identified Risks:**
    a. **Implement and Periodically Review Access Controls.** Warranty Solutions regularly evaluates who has access to customer information and their need to access it.
    b. **Assess Location and Nature of Data.** Warranty Solutions evaluates the collection, location, storage, and transmission of its data for security and resilience.
    c. **Encryption of Data**: All data transmitted over external networks is encrypted.
    d. **Assessments of Applications**: Warranty Solutions evaluates its internal and third-party developed applications for data security.
    e. **Use of Multi-Factor Authentication**: Warranty Solutions uses internal verification through at least two authentication factors.
    f. **Data Retention Management**: Warranty Solutions securely and in a timely manner disposes of personal data not in use as part of our information security program.
    g. **Change Impact Assessments**: Warranty Solutions assesses and anticipates its need to improve or change business processes, data management, and security protections as its operations change.
    h. **Monitoring Access to Customer Information**: Warranty Solutions maintains a log of user's activity in accessing customer information to monitor authorized access and detect unauthorized access.
4. **Staff Training:** Employees receive periodic training to enhance security awareness.
5. **Written Information Security Program/Policy**: Warranty Solutions has a written, comprehensive data security plan for Warranty Solutions that includes ensuring that our vendors are securing their data as required and conducting audits of vendors to confirm that fact. We believe the policy to be appropriate to the size, nature, and complexity of our business activities. Further Warranty Solutions has a written Incident Response Plan as part of that policy.
6. **Assessment of Data and Systems**: Warranty Solutions conducts periodic testing of its data security program. Penetration and vulnerability testing is performed annually.

If you have any further questions regarding our data security efforts, please contact us.

Sincerely,

Glenn Gardner
Chief Information Officer