SAFEGUARDS RULE CERTIFICATION

This Safeguards Rule Certification ("**Certification**") is provided to _____, and its Affiliates (collectively "**Dealer**") by Company in connection with services provided by Company to Dealer under a Services Agreement for the __ month period ending on _____ ("**Services**"). This Certification is provided in connection with such Services.

DEFINITIONS

1. **Affiliates** means any dealerships or business entities, under common control or ownership with Dealer, and authorized to sell or issue Company products or programs pursuant to the Dealer Agreement.
2. **Company** means the following entity or entities with which Dealer previously entered into a Services Agreement: iA American Warranty, L.P., Innovative Aftermarket Systems L.P., Service Guard Insurance Agency, L.P. dba Preferred Administrators, iA American Warranty Corp, Southwest Reinsurance Inc., or American Colonial Administration, LLC.
3. **Services Agreement** means the separate agreement entered into by Company and Dealer pursuant to which Company administers specific warranty, service contract or similar products or programs, sold or issued by Dealer to customers.
4. **Safeguards Rule** means the federal Gramm-Leach-Bliley Act ("**GLBA**") Safeguards Rule applicable to Dealer and any of its service providers with access to Dealer's "Customer Information" as defined in GLBA.

PHYSICAL & ADMINISTRATIVE PRACTICES

1. Company maintains a written information security program.
2. Company performs physical, administrative and electronic risk assessments relating to information safeguards at least annually.
3. Company performs training on security awareness for all employees at least annually.
4. Company has a cybersecurity insurance policy that covers data breaches affecting customer personal information we collect, receive, store or process on behalf of Dealer.
5. Company has a process and/or policy that limits the ability to request and access files (whether stored physically or electronically) containing customer personal information to only authorized individuals on a need-to-know basis.
6. Company provides mechanism for the secure destruction and disposal of documents containing customer personal information, such as locked shredding bins.
7. Company asks that each of our service providers and sub-processors sign a data processing agreement that complies with applicable state and federal data privacy laws.
8. Company has not experienced a data breach affecting customer personal information in the past 12 months.

ELECTRONIC & TECHNICAL PRACTICES

1. Company has an endpoint detection and response (EDR) software installed on all endpoint devices that is continuously monitored and managed.
2. Company performs automated backups of sensitive data or critical enterprise assets that are either stored offline or on segregated systems.
3. Company conducts social engineering and phishing simulations.
4. Company has performed penetration testing within the past 12 months.
5. Company regularly runs internal and external vulnerability scans.
6. Company stores network user credentials securely by ensuring such credentials are not stored in plain, readable text or in vulnerable format.
7. Company grants administrator privileges to our network and applications on a least-access, role-based, and need to know basis.
8. Company regularly updates and patches third-party software (e.g., antivirus, firewalls) and tests our network to ensure that such updates and patches have been successfully installed on all applicable devices.

COMPANY

By: _____

Typed Name: Katy Agnor

Title: CIO

Date: _____

V 202210