VW CREDIT, INC. THIRD-PARTY INFORMATION SECURITY POLICY

This VW Credit, Inc. Third-Party Information Security Policy ("Policy") applies if a third party ("Supplier") is providing services, products, or materials to VW Credit, Inc. ("VCI") that require VCI Data to be in Supplier's possession or under its control in connection with the agreement between VCI and Supplier (the "Agreement"). This Policy contains specific requirements relating to access of VCI Systems and VCI Data that Supplier, its personnel, and any of its affiliates or subcontractors must meet in its performance of the Agreement. This Policy is incorporated by reference into the Agreement.

1. Information Security Program Requirements

1.1 Information Security Program

Supplier will comply with, and remain in compliance with, at its expense:

- a final report ("SOC II Report") of the findings of a SOC II Type 2 review of all key software, network resources, computer systems, data, databases, or materials owned, operated, or controlled by on behalf of Supplier ("Supplier Systems") and internal operational controls to be used in connection with any information, confidential information, data, materials, works, expressions, or other content in written, electronic, or other form of media, including, but not limited to, all information and data about the customers (current, former or prospective) and employees (current, former or prospective) of VCI or its affiliates, or its affiliates customers', customers (current, former or prospective) or employees (current, former or prospective), and all intellectual property rights in that information and data created, generated, provided or submitted by, or on behalf of, VCI or its affiliates in connection with the Agreement ("VCI Data"). This review must be conducted by a reputable, independent external auditor reasonably acceptable to VCI (each, a "SOC II Review") together with a SOC II Type 2 certification by such auditor containing no material qualifications (each, a "SOC II Certification") or,

- ISO/IEC 27002 (Information Technology – Code of Practice for Information Security Management) ("ISO 27002"); or

- the VCI Information Security Requirements attached as Appendix 1 to this Policy (the "VCI Information Security Requirements").

1.2 In the event that Supplier stores, processes or transmits payment card primary account numbers or other cardholder data, Supplier also will, at its expense, be and remain in compliance with the then current Payment Card Industry Data Security Standard ("PCI DSS").

1.3 Information Security Certifications, Assessments and Reviews

- If Supplier elects to provide VCI with a SOC II Report of the findings of a SOC II Type 2 review, Supplier must, at its expense and on either an annual or bi-annual basis as

determined by VCI, conduct a SOC II Review and provide VCI with the resulting SOC II Report and SOC II Certification.

- If Supplier elects to demonstrate that it is and remains in full compliance with ISO 27002, Supplier must, at its expense, provide VCI with a certificate signed by an officer of Supplier certifying that it is in compliance with ISO 27002 on an annual basis.

- If Supplier elects to demonstrate that it is and remains in full compliance with the VCI Information Security Requirements, Supplier must, at its expense and on either an annual or bi-annual basis as determined by VCI, complete and provide VCI with an information security self-assessment ("ISSA").

- In the event that VCI, the ISSA, or the SOC II Report identifies any problem(s), Supplier will follow the process outlined in Section 3.

2. Supplemental Information Security Requirements

2.1 Access to VCI Data

- VCI is not obligated to allow Supplier access to VCI Data unless and until VCI is satisfied that Supplier is in compliance with this Policy.

- Supplier shall authenticate and permit access to VCI Data and VCI Systems only to authorized users pursuant to Sections 2.1 and 2.7.

- Supplier shall limit authorized users' access only to VCI Data and VCI Systems that they need to perform their duties and functions.

- Supplier shall require any individual accessing any VCI Data or VCI Systems to implement multi-factor authentication unless VCI's Chief Information Security Officer approves in writing the use of a reasonable equivalent or more secure access control.

- Supplier shall implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, VCI Data or VCI Systems.

- Supplier shall encrypt all VCI Data held or transmitted both in transit and at rest, using at least prevailing industry standard standards, and shall ensure any affiliate, subcontractor, or Supplier personnel processing VCI Data, will similarly encrypt VCI Data.

2.2 Incident Preparedness and Response Requirements

2.2.a Incident Response and Business Continuity and Disaster Recovery Plan

- Maintenance of a Written Incident Response Plan and a Business Continuity and Disaster Recovery Plan

  (1) Supplier must maintain a written Incident Response Plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of VCI Data or VCI Systems.

  (2) Supplier must maintain a written Business Continuity and Disaster Recovery Plan ("BCDR Plan") and have the capacity to execute the plan with respect to its primary and backup systems, resources and locations. The BCDR Plan will meet the following disaster recovery requirements: twenty-four (24) hour recovery time objective ("RTO") and four (4) hour recovery point objective ("RPO").

- Annual Incident Response Plan and BCDR Plan Review.

  (1) Supplier, at its expense and on an annual basis, must provide VCI with a summary of its current Incident Response Plan and BCDR Plan for VCI to review and approve.

  (2) If requested, Supplier must provide VCI, its auditors and other designees access to the full Incident Response Plan and BCDR Plan.

  (3) If requested, Supplier, at its expense, must revise its Incident Response Plan and BCDR Plan to address concerns identified by VCI and provide VCI with an updated version of the Incident Response Plan and BCDR Plan.

- Annual Incident Response Plan and BCDR Plan Tests

  (1) At least once a year, Supplier will perform Incident Response Plan and BCDR Plan tests and provide VCI with a written summary of the test results so VCI can assess the success of each test. Supplier will also give VCI the opportunity to participate in Supplier's annual Incident Response Plan and BCDR Plan tests on terms reasonably acceptable to Supplier.

  (2) On an annual basis, Supplier will provide VCI with a signed officer's certificate certifying that the Incident Response Plan and BCDR Plan are fully operational.

  (3) If VCI has any concerns related to either RTO or RPO requirements, then Supplier will promptly address VCI's concerns.

- Notice of Disaster

If the BCDR Plan must be enacted because of a disaster or event, then Supplier must promptly:

(1) notify VCI, as soon as reasonably practicable, of the disaster or other event; and

(2) provide VCI access to the services in a manner that is at least equal to the access provided to Supplier's other customers in connection with Supplier's performance of the Agreement.

- Annual VCI Disaster Recovery Rehearsal

If Supplier obtains, creates, generates, collects, has access to or processes Personal Information (as defined in the VW Credit, Inc. Privacy Policy) that is subject to any Privacy Laws (as defined in the VW Credit, Inc. Privacy Policy) in connection with Supplier's performance of the Agreement, then Supplier must, at its expense, participate in VCI's annual disaster recovery rehearsal.

2.2.b Security Event Notification and Reporting

- Supplier will notify VCI in writing within twenty-four (24) hours of any actual or reasonably suspected security event and/or unauthorized access of VCI Data affecting the confidentiality, integrity, or availability of VCI Data or Supplier Systems used to access software, network resources, computer systems, data, databases, or materials owned, operated, or controlled by VCI ("VCI Systems"). Such notice shall be delivered to: VCI-ITSecurity@vwcredit.com & VCIPrivacy@vwcredit.com.

- The notice of security event and/or unauthorized access provided to VCI must include:

(1) the reasonably expected impact of the security event and/or unauthorized access on VCI and its customers; and

(2) the remediation or corrective action to be taken with respect to Supplier Systems to prevent or mitigate any such security event and/or unauthorized access.

- Supplier must cooperate fully with VCI, regulatory or law enforcement agencies to investigate any such security event and/or unauthorized access. Supplier will be responsible for all costs and expenses related to such cooperation and investigation.

- Supplier agrees to take direction from VCI in the event any such security event necessitates reporting by VCI or any VCI affiliate or subcontractor to any Regulator (as defined in the VW Credit, Inc. Vendor Risk Management Policy) or to employees or customers of VCI or its affiliates or subcontractors.

- Supplier will provide VCI with the following written reports upon VCI's request:

- a summary of any security events and access violations to Supplier Systems that could affect VCI Data, together with a summary of any corrective action plans;

- a status report of any existing corrective action plans; and

a summary of the findings of any security vulnerability scan or penetration test that is performed with respect to the performance of the Agreement and Supplier Systems, including the perimeter, together with a summary of any corrective action plans prepared to address any identified vulnerabilities.

2.3 Storage, Return, or Destruction of VCI Data

- Supplier will accurately and completely collect and maintain information regarding the location and method of storage for all VCI Data.

- Prior to termination of the Agreement, or on a date otherwise specified by VCI, Supplier will meet with VCI representatives to prepare and implement a plan for the return of all VCI Data.

- In addition to Supplier's return or destruction obligations with respect to VCI Data under the Agreement, upon request or at termination of the Agreement, Supplier will:

  - return to VCI all VCI Data identified by VCI as returnable;

  - to the extent VCI Data cannot be returned to VCI, using any and all means (technical or otherwise) of overwriting and fully deleting all information/data to ensure that the deletion is permanent and the information/data cannot be retrieved, in whole or in part, by any means ("Securely Delete") electronic VCI Data from all media as soon as possible (excluding any VCI Data which is subject to a litigation hold request), and provide VCI with a certificate, signed by an officer of Supplier, certifying that this has been accomplished; or

  - to the extent that VCI Data cannot be so Securely Deleted, promptly provide a written description of the measures to be taken that will the continued protection of such VCI Data in compliance with the requirements of this Section and Supplier's confidentiality obligations.

2.4 Protection of VCI Data in the Event of Supplier Bankruptcy. If Supplier (a) files for bankruptcy, (b) becomes or is declared insolvent, (c) is the subject of any proceedings (not dismissed within thirty (30) days related to its liquidation, insolvency or the appointment of a receiver or similar officer, (d) makes an assignment for the benefit of all or substantially all of its creditors, (e) takes any corporate action for its winding-up, dissolution or administration, (f) enters into an agreement for the extension or readjustment of substantially all of its obligations, or (g) recklessly or intentionally makes any material misstatement as to financial condition, VCI will have the immediate right to take possession of all VCI Data then in the possession or under the

control of Supplier. VCI may retain the VCI Data until the trustee or receiver in bankruptcy or other appropriate court officer provides VCI with adequate assurances and evidence that the VCI Data will be protected from sale, release, inspection, publication or inclusion in any publicly accessible record, document, material or filing.

This Section 2.4 is a material term of this Policy, and VCI would not have permitted Supplier to access or use VCI Data without its inclusion.

2.5 Regeneration of VCI Data. Upon VCI's request, Supplier will promptly replace, regenerate, or obtain a new copy of any VCI Data handled or stored by Supplier that Supplier has lost or damaged. Alternatively, VCI may replace, regenerate, or obtain a new copy of any VCI Data that Supplier has lost or damaged, in which case, Supplier will promptly reimburse VCI for all reasonable costs associated with its efforts.

2.6 Vulnerability Assessments. Supplier will, at its expense and on an annual basis, have either a reputable third party or a dedicated separate internal team conduct an independent vulnerability assessment of all externally-facing Supplier Systems. Upon VCI's request, Supplier will provide VCI with evidence that the assessment has been performed and a summary of the critical and high risk findings from the assessment. Supplier will implement the recommendations set forth in any such assessment within ninety (90) days of finalization of the assessment, and, upon VCI's request, provide VCI with an update as to the status.

2.7 Information Security Requirements for Affiliates and Subcontractors

- Supplier must obtain VCI's prior written approval to provide access to VCI Data to any affiliate, subcontractor, or Supplier personnel of such affiliate or subcontractor.

- The subcontract with such affiliate or subcontractor must require the affiliate or subcontractor to comply with the applicable requirements under this Policy and any subcontractor restrictions set forth in the Agreement.

- If requested, Supplier will provide VCI with written evidence of its affiliate, subcontractor or Supplier personnel's compliance with these requirements.

- In the event that Supplier is unable to enter into a subcontract containing the minimum terms required with any affiliate or subcontractor, Supplier will, prior to transferring VCI Data to the affiliate or subcontractor:

  (1) evaluate such affiliate or subcontractor under Supplier's then current Vendor Risk Management Program (as defined in the VW Credit, Inc. Vendor Risk Management Policy);

  (2) provide VCI with a certificate, signed by an officer of Supplier, certifying that such evaluation has been completed and that any actions required to correct any identified deficiencies or problems have been

completed or are in the process of being completed in accordance with the corrective action plan established by:

(a) Supplier and such affiliate or subcontractor pursuant to the Vendor Risk Management Program; or

(b) Upon VCI's request, Supplier will provide VCI with a copy of the report prepared by Supplier in connection with any such evaluation.

3. Non-Compliance. In the event that Supplier is not in compliance with any requirements contained in this Policy, the VCI Information Security Policy or any information security requirements set forth in the Agreement; or

an SOC II Report identifies any problem(s) such that the auditor is unable to issue a SOC II Certification,

Supplier will, at its expense:

- prepare and provide VCI with a plan which must include, the responsible party and the specific planned actions to correct such problems within thirty (30) days from VCI's identification of the problem(s) or receipt of the SOC II Report identifying such problem(s);
- implement and complete the plan, as mutually agreed upon by the parties, within ninety (90) days from VCI's identification of the problem(s) or receipt of the SOC II Report identifying such problem(s); and
- keep VCI updated with status reports during the implementation of the plan.

APPENDIX 1 TO
VW CREDIT, INC. THIRD-PARTY INFORMATION SECURITY POLICY

All Supplier team members, employees, contractors, and agents are responsible for implementing and observing the following VCI Information Security Requirements within their respective areas of responsibility.

- Supplier has established, and will maintain during the term of the Agreement, commercially reasonable administrative, physical, and technical safeguards for the protection of VCI Data, VCI System, and Supplier Systems commensurate with industry standards for similar services, and maintain reasonable measures for preventing the destruction, loss, misuse, unauthorized access, disclosure or alteration of VCI Data, VCI System, and Supplier Systems including regular back-ups, security and incident response protocols, and application and infrastructure monitoring, that are no less rigorous than the prevailing industry standards with respect to data security and data privacy and otherwise required under applicable data protection laws.

- Supplier shall maintain an Acceptable Use and End User Policy for all Supplier Systems.

- Supplier shall maintain policies and processes to include information security when recruiting, hiring, onboarding, and terminating Supplier personnel. Supplier shall provide such policies and procedures at least thirty (30) days after the Agreement's effective date and provide such policies to VCI at least annually. All individuals who access VCI Data must be aware of the information security responsibilities under these Requirements.

- Supplier shall restrict access to Supplier facilities and non-public areas of any such locations to Supplier personnel who are authorized by Supplier and deemed necessary by Supplier for Supplier's performance of its obligations under the Agreement.

- Supplier shall ensure access to VCI Systems and VCI Data is authorized in writing by VCI.

- Supplier shall develop Supplier Systems and changes to Supplier Systems using a defined methodology and implement utilizing prevailing industry security controls.

- Supplier shall establish security monitoring processes that enable the identification of information security incidents and the measurement of the security condition of VCI Data.