CISCO
CREDIT INFORMATION SERVICE COMPANY

CISCO Credit Services Agreement

Company Information			
Company Name:			
Address:	City:	State:	ZIP:
Phone:	Fax:		
Type of Ownership: ☐ Partnership	☐ Sole Owner	☐ Corporation	☐ LLC
Do you have any other DBA's? ☐ Yes	☐ No	If Yes, please list:	
Federal Tax ID:	Years of Operation:		
Do you own or lease the building in which you are located?	☐ Own	☐ Lease	
Lease/Management Co. Name & Contact Number:	Name:	Phone:	
Number of employees at this branch:	Number of Branches:	Total Employees:	
Estimated # of credit reports you will access monthly:			
Do you already have a Credit Reporting Agency? ☐ Yes	☐ No	If Yes, please list:	
Responsible Party's name and driver's license number:			
Responsible Party's email address:			
Company Website:			

Business Information			
Business Checking Info			
Bank:	Account #:	Phone #:	
Billing Information (if different from above)			
Address:	City:	State:	ZIP:
Phone:	Email:		
Indicate which Pricing you want your account billed under:	☐ Bundle	☐ Standard	
*note: If nothing is checked, your account will automatically be billed under the Standard pricing			
Business References (to confirm your business as a mortgage company)			
Name:	Company:	Phone#:	
Name:	Company:	Phone#:	

Additional Information		
Will reports be used for mortgage purposes only?	☐ Yes	☐ No
Is the actual company operated from a residence?	☐ Yes	☐ No
Have you filed for bankruptcy in the last 10 years?	☐ Yes	☐ No
Is your company a publicly traded company?	☐ Yes	☐ No

Payment Information

1. The undersigned Client hereby petitions CISCO Credit (CISCO) to render service in accordance with its customary practices, for which the Client agrees to pay promptly on billing by CISCO the fees provided herein.
    a. Payments are due net within 30 days, a 3% monthly charge applies to balances remaining after 30 days. In the event that legal action is required to recover any outstanding balances the undersigned client agrees to pay all fees associated with the balance recovery. The undersigned client accepts personal responsibility of any outstanding balance and all collection charges up to 50% of the outstanding balance. In the event that an outstanding balance is turned over to a collection agency, a minimum $300.00 collection charge will be added to the outstanding balance. Accessing any of the three credit repositories will result in a charge. All transaction charges for products or services are reflected on each credit report and invoice. The undersigned grants permission to CISCO to access the three national repositories for the purpose of this application. CISCO Credit reserves the right to suspend service due to lack of payment. The Client is responsible for any reports pulled and will be billed accordingly. The Client understands that if the CISCO system is used improperly by company personnel, or if their access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of the undersigned clients company, they may be held responsible for financial losses, fees, or monetary charges that may be incurred and that their access privilege may be terminated.
    b. The Client agrees to a monthly minimum requirement of orders totaling at least $25.00. In the event that the client does not order a minimum of $25.00 of orders during the monthly billing period they will be billed either the full $25.00 monthly minimum or the difference between their orders in the month and the monthly minimum
2. The undersigned Client will comply with all the provisions of the Public Law 91-508 (Fair Credit Reporting Act), LexisNexis policies, and all other applicable federal and state statutes. The undersigned recognizes its responsibilities there under, and acknowledges receipt of the notice set forth in Exhibit A attached hereto.
3. The undersigned Client certifies that all inquiries will be made only when the client intends to use the information in connection with a legitimate mortgage transaction involving a consumer and that it is not one of the businesses listing on Exhibit B attached within the appendix. Furthermore, all products including but not limited to credit reports, and all LexisNexis products will be used solely for mortgage related purposes.
4. The undersigned Client herby petitions CISCO to render service regarding the reissuance or secondary use of consumer reports in accordance with its customary practices and will be billed accordingly. The undersigned client agrees, represents, and warrants that it is a mortgage lender/broker and in using the services of CISCO, the client agrees to comply with the provisions of 15 U.S.C §1681 *et seq.* ("FCRA") and that services will be requested only for the Client's exclusive use.
5. The undersigned certifies that consumer reports will be ordered and used only in connection with credit transactions involving consumers on whom the information is to be furnished and involving the extension of credit to, or to review or collect an account of the consumer, even though otherwise permitted by law. The client may reissue or share such report with one or more credit grantors which (1) have permissible purpose under the FCRA to receive such reports and (2) are "Qualified Subscribers" of CISCO. A "Qualified Subscriber" is a user of CISCO that has signed a service agreement with CISCO. The reissuance or sharing of a consumer credit report with a Qualified Subscriber, may be accomplished by the physical sharing of a copy of the report or by obtaining another copy from CISCO. In either even, the undersigned agrees to inform CISCO of any such reissues and to pay the fees as per payment agreement net within 30 days.
6. The undersigned Client certifies that its organization is a bona fide business and that it has read and will adhere to the Access Security Requirements attached hereto and made a part hereof. The national repositories require that Client maintain copies of written authorization for credit inquiries and LexisNexis products for five years. Client agrees to notify CISCO immediately of any change in business location or changes in personnel.
7. No information furnished to the undersigned client is guaranteed, nor is CISCO, the national repositories, or LexisNexis responsible for such information. CISCO shall not be responsible or liable in any manner whatsoever for any loss or injury to the undersigned client resulting from the obtaining or furnishing of such information, and shall not be deemed to have guaranteed the accuracy of such information.
8. Client hereby agrees to comply with all policies and procedures instituted by CISCO and required by CISCO's

consumer reporting vendors. CISCO will give Client as much notice as possible prior to the effective date of any such new policies required in the future, but does not guarantee that reasonable notice will be possible. Client may terminate this agreement at any time after notification of a change in policy in the event Client deems such compliance as not within its best interest. Client recognizes that is has separate responsibilities related to each of the national repositories set forth in Appendix A-1, Appendix A-2, Appendix A-3, Appendix B, Appendix C-1 and C-2, all of which are attached hereto.

9. The undersigned client hereby authorizes CISCO to provide copies of any information regarding the client to CISCO's consumer report vendors.
10. The client agrees that CISCO and CISCO's consumer report vendors including LexisNexis, shall have the right to audit records of the client that are relevant to the provision of services set forth in this agreement. CISCO may utilize a third-party vendor to perform an on-site inspection of Client's business, and Client agrees to allow access to such third party. Client further agrees that it will respond within the requested time frame for information requested by CISCO's consumer reporting vendors regarding information provided by such vendor. The client understands that such vendor may suspend or terminate access to the vendor's information in the event that the Client is not in compliance with applicable law, this agreement, or if Client does not cooperate with any such investigation.
11. Client agrees to notify CISCO of any change of ownership, control, or address change fifteen days prior to any such change. CISCO may require the new ownership to re-apply for the services provided herein and may require a new physical inspection in the event that the office location is changed. CISCO will provide, and the Client will utilize, training and training materials to the Client in order for the Client to comply with the federal Fair Credit Reporting Act and with the policies and procedures required by CISCO's consumer reporting vendors.
12. 168115 U.S.C. *et seq* also requires certain other responsibilities of Clients whom access consumer credit reports from consumer credit reporting agencies. Those responsibilities are attached, and made a part hereof as Exhibit A to this agreement. The FCRA provides that any person who knowingly and willfully obtains information on a consumer reporting agency under false pretenses shall be fined under title 18, or imprisoned for no more than two years, or both.

Terms Related to Credit Scoring Services

1. Based on an agreement with the national repositories (Experian/TransUnion/Equifax) and Fair Isaac Corporation ("Fair Isaac"), the Client has access to a unique and proprietary statistical credit scoring service jointly offered by the national repositories and Fair Isaac which evaluates certain information in the credit reports of individual consumers from the national repositories data bases ("Scoring Systems") and provides a score which rank orders consumers with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring ("the Score").
2. The client from time to time may desire to obtain Scores from the national repositories via an online mode in connection with consumer credit reports
3. The client has previously represented and now, again represents that it is a Mortgage credit company and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Report Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").
4. The client certifies that it will request Scores pursuant to procedures prescribed by CISCO from time to time only for the permissible purpose certified above and will use the Scores obtained for no other purpose.
5. The client will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.
6. Client agrees that it shall use each score only for a one-time use and only in accordance with its permissible purpose under FCRA.
7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, CISCO may, upon its election, discontinue service the Client and cancel this Agreement in whole or in part with ten

(10) days prior written notice of termination of this Agreement to the party (e.g. the services provided under this Addendum only) immediately.

8. Client recognizes that factors other than the Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors.
9. The national repositories and Fair Isaac shall be deemed third party beneficiaries under this Addendum
10. Up to five score reason codes, or if applicable, exclusion reasons, are provided to Client with Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher score, and may be disclosed to consumers as reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg B"). However, the score itself is proprietary to Fair Isaac or its producer, and may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party except:
    a. to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes.
    b. As clearly required by law.
11. Client will not publicly disseminate any results of validations or other reports derived from the Scores without Fair Isaac and the national repositories' prior written consent.
12. In the event that the Client intends to provide Scores to any agent, Client may do so provided, that Client first enters into written agreement with such agent that is consistent with Client's obligations and acknowledgments of the agent:
    a. Such agent shall utilize the Scores for the sole benefit of the Client and shall not utilize the Scores for any other purpose including for such agent's own purpose or benefit.
    b. That the Score is proprietary to the producer or to Fair Isaac and accordingly, shall not be disclosed to the credit applicant or any third party without prior written consent from the national repositories' and Fair Isaac except
        i. To credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes.
        ii. As clearly required by law.
    c. Such agent shall not use the Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration.
    d. Such agent shall not resell the Scores.
    e. Such Agent shall not use the Scores to create or maintain a database for itself or otherwise.
13. Client acknowledges that the Scores provided under this Agreement which utilize, and individual's consumer credit information will result in an inquiry being added to the consumer's credit file.
14. Client shall be responsible for compliance with all applicable federal or state legislations, regulations, and judicial actions as now or as may become effective, including but not limited to, the FCRA, the ECOA, the Reg B., to which it is subject.
15. The information including, but not limited to, the consumer credit data used in providing Scores under this Agreement were obtained from sources considered to be reliable. However due to the possibilities of errors inherent in the procurement and compilation of data in the procurement and compilation of data involving a large number of individuals, neither the accuracy, nor completeness of such information is guaranteed. Moreover, in no event shall the national repositories, Fair Isaac, nor their officers, employees affiliated companies or bureaus, independent contractors, or agents be liable to Client for any claim, injury, or damage suffered directory or indirectly by the Client as a result of the inaccuracy or incompleteness of such information used in providing Scores under this Agreement and/or as a result of Client's use of Scores and/or any other information or service provided under this Agreement.
16. Fair Isaac and other Score producers, warrant that the scoring algorithms as delivered to the national repositories and used in the computation of the Score Models are empirically derived from the national repositories' credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm uses a "prohibited basis" as that

term is defined in the Equal Credit Opportunity Act (ECOA) and Reg B promulgated there under. The score may appear on a credit report for convenience only but is not a part of the credit report nor does it add to the information in the report on which it is based.

a. The warranties set forth in section 15.1 are the sole warranties made under this addendum concerning the scores and any other documentation or other deliverables and services provided under this agreement. And neither Fair Isaac nor the national repositories make any other representations or warranties concerning the products and services to be provided under this agreement other than as set forth in this addendum. The warranties and remedies set forth in section 15.1 are in lieu of all others, whether written or oral, expressed or implied, including but not limited to warranties that might be implied from a course of performance, dealing, or trade usage. There are no implied warranties of merchantability or fitness for a particular purpose.

17. In no event shall any party be liable for any consequential, incidental, indirect, special, or punitive damages incurred by the other parties and arising out of the performance of this agreement, including but not limited to loss of good will and lost profits or revenue, whether or not such loss or damage is based in contract, warranty, tort, negligence, strict liability, indemnity, or otherwise, even if a party has been advised of the possibility of such damages. These limitations shall apply not withstanding any failure of essential purpose of any limited remedy.
18. The foregoing notwithstanding, with respect to subscriber, in no event shall the forecasted limitations of liability, set forth above in section 16, apply to damages incurred by TransUnion and/or Fair Isaac as a result of: (a) Governmental regulatory or judicial action(s) pertaining to violations of FCRA and/or other laws, regulations and/or judicial actions to the extent such damages result from client's breach, directly or through client's agent(s), of its obligations under this agreement.
19. Additionally, neither the national repositories nor Fair Isaac shall be liable for any and all claims arising out of or in connection with this addendum brought more than one (1) year after the cause of action has occurred. In no event shall the national repositories' and Fair Isaac's aggregate total liability, if any, under this agreement, exceed the aggregate amount paid under this addendum by client during the twelve (12) month period immediately preceding any such claim, or ten thousand dollars ($10,000.00) whichever amount is less.
20. This addendum may be terminated automatically and without notice:
    a. in the event of a breach of the provisions of this Addendum by the client
    b. in the event the agreement(s) related to the Scoring System between the national repositories, Fair Isaac and the Client are terminated or expire
    c. in the event the requirements of any law, regulation or judicial action are not met
    d. as a result of changes in law, regulations or regulatory or judicial action that the requirements of any law, regulation, or judicial action will not be met
    e. the use of the Scoring system is the subject of litigation or threatened litigation by any governmental entity.
21. Death Master File: Access to the Death Master File as issued by the Social Security Administrations requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R § 1110.102(a)(1). All end users must certify that they will not take any adverse action against any consumer without further investigation to verify information from the deceased flag or other indicia from the Experian data.

Term Related to Privacy Disclosure

1. CISCO Does not resell or share any information provided by clients with third parties.
2. Client certifies that all scores and reason codes whether oral or written shall be maintained by the Client in strict confidence and disclosed only to employees whose duties reasonably relate to the legitimate business purpose for which the report is requested and will not sell or otherwise distribute to third parties any information received there under, except as other required by law.
3. Unless explicitly authorized in this Agreement or in a separate agreement between CISCO and the Client or as explicitly otherwise authorized in advance and in writing by a national repository through CISCO, the Client shall not disclose to consumers or any third party, any or all scores provided under this Agreement, unless clearly required by law.

4. Client shall comply with all applicable laws and regulations in using the Scores and reason codes.
5. The Client, its employees, agents, and subcontractors shall not use the trademarks, services marks, logos, names, or any other proprietary designations, whether registered or unregistered to any party involved in the provision of the Experian, TransUnion, Equifax, or Fair Isaac Model without such entities prior written consent.
6. The Client shall not attempt, in any manner, directly, or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by any of the national repositories or score producers.
7. Experian, TransUnion, Equifax, and Fair Isaac have warranted to CISCO that that the Experian/Fair, Isaac Model is empirically derived and is demonstrably and statistically sound and that to the extent the population to which the Experian, Trans Union, Equifax, and Fair Isaac Model is applied is similar to the population sample on which the Experian/Trans Union/ Equifax/Fair Isaac Model was developed, the Experian/Trans Union/ Equifax/Fair Isaac Model score may be relied upon by CISCO and/or Client to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Client. Experian/Trans Union/ Equifax/Fair Isaac further warrants that so long as they provide the Experian/Fair, Isaac Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 et seq. The foregoing warranties are the only warranties Experian/Trans Union/ Equifax/Fair Isaac have given CISCO with respect to the Experian/Trans Union/ Equifax/Fair Isaac Model and such warranties are in lieu of all other warranties, express or implied, Experian/Fair Isaac might have given broker and/or end users with respect thereto, including for example, warranties of merchantability and fitness for a particular purpose. Client's rights under the foregoing warranty are expressly conditioned upon Client's periodic revalidation of the Experian/Trans Union/ Equifax/Fair Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR section 202 et seq.)The aggregate liability of Experian/Trans Union/ Equifax/Fair Isaac to each End User shall not exceed the lesser of the Fees paid by Broker to Experian/Fair, Isaac, the fees paid by the End User during the six (6) month period immediately preceding the Client's claim, or the fees paid by the pertinent End User to our company during said six (6) Month period, and excluding any liability of Experian/Fair, Isaac for incidental, indirect, special or consequential damages of any kind.

Credit Scoring Services

Whereas, provider is an authorized reseller of Experian Information Solutions, Inc. ("Experian"); and, Experian and Fair Isaac Corporation ("Fair Isaac") offer the "Experian/Fair Isaac Model", consisting of the application of a risk model developed by Experian and Fair Isaac, which employs a proprietary algorithm which when applied to credit information relating to individuals with whom the Client contemplates entering in to a credit relationship with will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

Therefore, for good and valuable consideration and intending to be legally bound, the Client and Provider which will be referred to as "CISCO" hereby agree as follows

General Provisions:

1. The subject of this Agreement is the End User's purchasing of Scores produced from Experian/Fair Isaac Model from CISCO. This agreement will apply to all uses of the Experian/Fair Isaac Model by the Client during the term of this agreement. Under this agreement during its terms, CISCO will provide the Client with the Scores upon request.

Experian/Fair Isaac Scores

1. The client warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the federal Equal Credit Opportunity Act, 15 USC Section 1691 et seq. or

Regulation B promulgated thereunder. The foregoing warranties are the only warranties CISCO has given the Client with respect to the Scores. Such warranties are in lieu of all other warranties, express, or implied that CISCO might have given to the Client.

2. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.)
3. The client hereby releases and holds harmless CISCO, Fair Isaac, Experian, and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of liability for any damages, losses, costs, or expenses, whether directly or indirectly suffered or incurred by the Client resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

Intellectual Property

1. Nothing in this agreement shall be deemed to grant the Client any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by CISCO, Experian, Fair Isaac, or any third party involved in the delivery of the scoring services hereunder.
2. The client acknowledges that the Experian/Fair Isaac Score Model and its associated intellectual property rights in its output are the property of Fair Isaac.
3. By providing the Scores to the Client pursuant to this Agreement, CISCO grants to the Client a limited license to use information contained in reports generated by the Experian/Fair Isaac Model solely in its own business with no rights to sublicense or otherwise sell or distribute said information to third parties. Before directing CISCO to deliver Scores to any third party as may be permitted by this Agreement, the Client agrees to enter into a contract with said third party that (1) limits the use of the Scores by the third party only to the use permitted to the Client and (2) Identifies Experian and Fair Isaac as express third-party beneficiaries of such contract.
4. The Client shall not use, or permit its employees, agents, and subcontractors to use the, trademarks, service marks, logos, names, or any other proprietary designations of CISCO, Experian, Fair Isaac, or their respective affiliates whether registered or unregistered without such party's prior written consent.

Compliance and Confidentiality

1. In performing this Agreement and in using information provided hereunder, the Client shall comply with all Federal, State, and Local statutes, regulations, and rules applicable to consumer credit information, LexisNexis policies, and nondiscrimination in the extension of credit from time to time in effect during the term of this agreement. The Client certifies that
    a. It has permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute.
    b. Any use of the Scores for the purpose of evaluating the credit risk associated with applicants, prospects, or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act.
    c. The Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the Client along with the Scores.
2. The Client will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. The Client will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, the Client will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of the Client and while in transport between the parties. The Client certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair Isaac's express without written permission.

3. Under no circumstances will the Client attempt in any manner, directly, or indirectly, to discover, or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair Isaac in performing the Scoring services hereunder.
4. Notwithstanding any contrary provision of this Agreement, the Client may disclose the Scores provided to the Client under this Agreement (1) to credit applicants when accompanied by the corresponding reason codes in the context of bona fide lending transactions and decisions only. (2) as clearly required by law.

Indemnification and Limitations

1. The Client will indemnify, defend, and hold CISCO, Experian, and Fair Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses including but not limited to attorneys' fees arising out of or resulting from any nonperformance by the Client of any obligations to be performed by the Client under this Agreement, provided that Experian/Fair Isaac have given the Client prompt notice of, and the opportunity and the authority but not the duty to defend or settle any such claim.
2. Notwithstanding any other provision of this agreement, under no circumstances will CISCO, Experian, or Fair Isaac have any obligation or liability to the Client for any incidental, indirect, special, or consequential damages incurred by the Client, regardless of how such damages arise and of whether or not the Client was advised such damages might arise. In no even shall the aggregate liability of CISCO, Experian, or Fair Isaac to the Client exceed the fees paid by the Client pursuant to this agreement during the six-month period immediately preceding the date of the Client's claim.

Miscellaneous

1. The Client acknowledges that the Scores results from the joint efforts of Experian and Fair Isaac. The client further acknowledges that each Experian and Fair Isaac have a proprietary interest in said Scores and agrees that either Experian or Fair Isaac may enforce those rights as required.
2. This Agreement sets forth the entire understanding of the Client and CISCO with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties whether oral, or written by any officer, employee, or representative of either party relating thereto.

I have read and understand the enclosed – Access Security Requirements for Reseller End-Users for FCRA and GLB 5A Data

Signature:_____

Print Name: _____

Title: _____

Date:_____

Appendix A-3

Equifax Requirement: VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

The undersigned_____("Customer"), acknowledges that it subscribes to receive various information serviced from Equifax Credit Information Services, Inc. ("Equifax") in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts. In connection with Customer's Continued use of Equifax information services in relation to Vermont consumers, Customer hereby certifies as follows:

Vermont Certification. Customer certifies that it will comply with applicable provisions under Vermont law. In particular, Customer certifies that it will order information services relating to Vermont residents, that are credit reports as defined by the VFCRA, only after Customer has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules.

Customer/Company Name: _____

Signature: _____

Printed Name and Title_____

Date: _____

Account Number_____

Please Also Include the Following Information:

Compliance Officer or Person Responsible for Credit Reporting Compliance

Name: _____

Title: _____

Mailing Address: _____

Email Address: _____

Phone: _____

Fax: _____

Customer: Maintain a copy for your records.

Applicable Law

The validity, construction, and performance of this Agreement shall be governed by and construed in accordance with the laws of the State of Arizona, excluding that body of law applicable to choice of law. The parties consent and submit to the jurisdiction and venue of the state and federal courts located in Maricopa County of the State of Arizona to determine the validity, construction and performance of this Agreement.
In Witness hereof, the undersigned herby signs this Agreement as of the following date:

_____/____/_____(Date)

Signature: _____ Print Name: _____

Title: _____ Email: _____

Social Security: _____ Company Name: _____

Home Address: _____ State, City, Zip: _____

Phone Number: _____ Home Fax: _____

Co-Signer Section Below (complete if applicable)

Signature:_____ Print Name:_____

Title: _____ Email: _____

Social Security: _____ Company Name:_____

Home Address: _____ State, City, Zip: _____

Phone Number: _____

CISCO CREDIT, INC.

By: _____

Name: _____

Title: _____

Access Security Requirements for Reseller End-Users for FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to systems or data through CISCO Credit, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. CISCO Credit reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing CISCO Credit services, Company agrees to follow these Experian security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian data:

1. Implement Strong Access Control Measures

1.1 Certify that the client shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Reseller must use the complete entire wording stated above or language substantially similar within the contract with the end user.

1.2 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from will ever contact you and request your credentials.

1.3 If using third party or proprietary system to access CISCO Credit systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing our data/systems.

1.4 If the third party or third party software or proprietary system or software, used to access CISCO Credit data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.5 Create a unique user ID for each user to enable individual authentication and accountability for access to CISCO Credit infrastructure. Each user of the system access software must also have a unique logon password.

1.6 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.7 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.8 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.9 Passwords (e.g. user/account password) must be changed immediately when:

- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.10 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all enduser (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm are utilized (e.g. AES 256 or above). Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30 minute inactive session timeout.

1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of the membership application.

1.13 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.

1.15 Implement a process to terminate access rights immediately for users who access Experian credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. <u>Maintain a Vulnerability Management Program</u>

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.

- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. <u>Protect Data</u>

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. <u>Maintain an Information Security Policy</u>

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify CISCO Credit within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with the

Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is Company's responsibility to ensure the service provider is engaged with Experian and an exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

5. <u>Build and Maintain a Secure Network</u>

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access CISCO Credit systems, access to third party tools/services must require multi-factor authentication.

6. <u>Regularly Monitor and Test Networks</u>

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access CISCO Credit systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

7. Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
    - ISO 27001 ○ PCI DSS ○ EI3PA
    - SSAE 16 – SOC 2 or SOC3 ○ FISMA
    - CAI / CCM assessment

8. General

8.1 CISCO may from time to time audit the security mechanisms Company maintains to safeguard access to Experian information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to CISCO upon request, audit trail information and management reports generated by the vendor software, regarding Company individual authorized users.

8.3 Company shall be responsible for and ensure that third party software, which accesses CISCO information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses CISCO information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example:
static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access CISCO systems shall be made available to CISCO upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to CISCO must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Repositories to CISCO within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to CISCO of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-804-0043, Email notification will be sent to support@ciscocredit.com.

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to CISCO services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of CISCO networking and computing resources may be monitored and audited by CISCO, without further notice.

8.10 The undersigned hereby provides permission for CISCO Credit to email all addresses/domains owned by the undersigned company with any updates or marketing features.

8.11 Company acknowledges and agrees that it is responsible for all activities of its employees/authorized users, and for assuring that mechanisms to access CISCO services or data are secure and in compliance with its membership agreement.

8.12 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by CISCO.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to CISCO provided services via Internet ("Internet Access").

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with CISCO on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to CISCO provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each CISCO product based upon the legitimate business needs of each employee. CISCO shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by CISCO. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). CISCO approval of requests for (Internet) access may be granted or withheld in its sole discretion. CISCO may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. An officer of the Company agrees to notify CISCO in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with CISCO on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with CISCO on information and product access, in accordance with these Experian Access Security Requirements for Reseller EndUsers. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head
   Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to CISCO systems and information (via the Internet).
   Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to CISCO immediately.
2. As a Client to CISCO products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to CISCO product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will

generally be available during normal business hours and can liaise with CISCO Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding CISCO representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access CISCO products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to CISCO regarding access to CISCO products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to CISCO
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with CISCO when needed on any system or user related matters.

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.

ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.

PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Exhibit A

FCRA PERMISSIBLE PURPOSE CERTIFICATION

In contracting for the services under this Agreement, Customer is a "User" of "Consumer Reports" as those terms are defined under the FCRA, and as such certifies as follows:

1. The nature of User's business is: _____

2. User orders Consumer Reports [Reseller] for the following purpose(s) under the Fair Credit Reporting Act and such reports will not be used for any other purpose:

Please check **all** that apply:

- ☐ For the extension of credit to the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(A).
- ☐ For the review of an account of the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(A).
- ☐ For the collection of an account of the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(A).
- ☐ For use in connection with the underwriting of insurance involving the consumer in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(B).
- ☐ For use, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation in accordance with 15 U.S.C. Sec.1681(b)(a)(3)(E).
- ☐ In connection with the assessment of the consumer's ability to pay for a medical care transaction initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681(b)(a)(3)(F)(i).
- ☐ In connection with a rental car transaction where the transaction is initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681b(a)(3)(F)(i).
- ☐ In connection with a demand deposit account or related new account opening transaction where the transaction is initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681b(a)(3)(F)(i).
- ☐ In response to a request by the head of a State or local child support enforcement agency (or a State or local government official authorized by the head of such an agency). In accordance with 15 U.S.C. Sec. 1681(b)(a)(4), Customer makes the following certifications:

  (A) the consumer report is needed for the purpose of establishing an individual's capacity to make child support payments or determining the appropriate level of such payments;

  (B) the paternity of the consumer for the child to which the obligation relates which has been established or acknowledged by the consumer in accordance with State laws under which the obligation arises (if required by those laws);

(C) the Customer has provided at least 10 days' prior notice to the consumer whose report is requested, by certified or registered mail to the last known address of the consumer, that the report will be requested; and

(D) the consumer report will be kept confidential, will be used solely for a purpose described in subparagraph (A), and will not be used in connection with any other civil, administrative, or criminal proceeding, or for any other purpose.

☐ For use in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(D).

☐ With express written instructions of the consumer for reasons **other than** an employment purpose in accordance with FCRA Section 15 U.S.C. Sec. 1681(b)(a)(2).

If you have selected "with express written instructions of the consumer" above, please specify intended use:

_____

3. The Federal Fair Credit Reporting Act imposes criminal penalties – including a fine, up to two years in prison, or both – against anyone who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses, and other penalties for anyone who obtains such consumer information without a permissible purpose.

This certification supersedes any pre-dated certifications.

I hereby certify that I have direct knowledge of the facts stated above and that I am authorized to execute this certification on behalf of the company listed above.

By:

_____
(Signature)

Name:

_____
(Printed or Typed)

Title:

_____

Date:

_____

Rev. 12.28.2021

ADDENDUM TO CISCO CREDIT AGREEMENT FOR SERVICE

This Service Addendum, which is dated and effective the _____day of _____, 20_____. In addition to all other requirements in the Agreement between the signer and CISCO Credit, as amended, pertaining to the access to and use of FICO scores, the following conditions shall govern Subscriber's access to and use of FICO Resilience Index (FRI):

Limitations on Use. Subscriber shall only use FRI when the FRI Score is pulled simultaneously with another FICO Score (i.e., dual processing where such Scores are pulled on the same consumer record for the same date as part of the same Score pull), solely for the Subscriber's internal business purposes and in support of the Subscriber's (i)credit evaluations (for the permitted business-to-business purpose for which the additional FICO Score was pulled), and (ii) evaluation of its ongoing use of FRI for such purposes and for no other purpose.

The FRI must be calculated on the same records and for the same date as the corresponding additional FICO Score.

Customer/Company Name: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Rev. 12.28.2021

Repository Compliance Form

Please List Your Companies End Users for Bureau Compliance

*An “End User” is anyone in the lending process that will at any point receive a copy of the credit report or scores either electronically or on paper

Please list the information requested below for each of the wholesale, correspondents, or other lenders that your company does business with that may come into possession of a credit report that you have ordered during the lending process.

Lender/ Contact Name/ Address/ City/ State/ ZIP/ Phone

CISCO
CREDIT INFORMATION SERVICE COMPANY

Rev. 12.28.2021

2815 S. Alma School Rd. Ste 109
Mesa, AZ 85210
480-491-6001 / 800-804-0043

CREDIT CARD AUTHORIZATION

RIGHT TO CHARGE CREDIT CARD FOR PAYMENTS: (Required)

The undersigned acknowledges that the services will be billed monthly and that the bills are due and payable in full upon receipt. In the event that you fail to pay charges billed on your monthly Cisco Credit bill, or Cisco Credit is unable to bill you, Cisco Credit shall have the immediate right to bill outstanding sums to your credit card. Cisco Credit may assign unpaid late balances to a collection agency for appropriate action. In the event legal action is necessary to collect on balances due, you agree to reimburse Cisco Credit for all expenses incurred to recover sums due, including attorney's fees and other legal expenses.

Print Name _____ Signature _____ Date _____

RIGHT TO CHARGE CREDIT CARD FOR SETUP FEE: (Required)

I authorize Cisco Credit to charge my credit card in the amount of $85 as payment for the setup fee. The undersigned acknowledges that there is a setup fee on all accounts and the fee must be paid in advance and is non-refundable. By signing this document, you are agreeing not to dispute or cancel this charge. A faxed copy of this authorization and the undersigned signature may be deemed equivalent to the original and may be used as a duplicate original.

Print Name _____ Signature _____ Date _____

RIGHT TO CHARGE CREDIT CARD ON A MONTHLY BASIS: (Optional)

The undersigned authorizes Cisco Credit to charge the credit card set forth below on the billing invoice date for the balance due of the company. By signing this document, you are agreeing not to dispute or cancel this charge. A faxed copy of this authorization and the undersigned signature may be deemed equivalent to the original and may be used as a duplicate original.

Print Name _____ Signature _____ Date _____

NAME AS IT APPEARS ON THE CARD: Company Name

BILLING ADDRESS

CITY STATE ZIP

CREDIT CARD NUMBER EXP.DATE CVV

Please Indicate: _____ Debit Card _____ Credit Card

NOTE: A 3% Convenience fee will be charged on all Credit Card invoice payments

Businesses that Cannot Be Provided Credit Information

- Adoption Search Firms
- Asset Location Services (not including collection agencies or with respect to GLBA information)
- Attorney/Law Firms
- Bail Bond Enforcement / Bounty Hunters
- Check Cashing
- Child Location Services
- Condominium/Homeowners Associations
- Country Clubs
- Credit Counseling – For Profit
- Credit Repair Companies or Credit Clinics
- Dating Services
- Determination of whether or not to file a personal lawsuit/judgement against the subject of the data
- Diet Centers
- Financial Counseling – except a registered securities broker dealer or a certified financial planner
- Future Services (i.e. Continuity Clubs)
- Foreign Company or Agency of a Foreign Government
- Genealogical or Heir Search Firm
- Individuals Seeking Information for Private Use
- Insurance Claims
- Internet People Locator Services
- Investigative Companies including Private Investigators and Detective Agencies
- Law Enforcement
- Loan Modification Companies
- Marketing Companies
- Massage Services
- Media Agencies, News Agencies, Journalists, or Subscription Based Services
- Non-Government Agencies or businesses Associated with the Collection of Child Support
- Paralegals
- Pawn Shops
- Pornography – Companies Involved and or Associated with Inappropriate Adult Content Web Sites and or Adult Type Telephone services
- Spiritual Counseling Companies
- Tattoo Service
- Timeshares (unless proof of credit extension is procured)

CISCO
CREDIT INFORMATION SERVICE COMPANY

Rev. 12.28.2021

2815 S. Alma School Rd. Ste 109
Mesa, AZ 85210
480-491-6001 / 800-804-0043
www.ciscocredit.com

Sample Letter of Intent

Trans Union Setup Requirement

Letter of Intent

"XYZ" Mortgage is a Mortgage Broker / Banker.

The intent of the credit reports is mortgage applications.

Our anticipated volume is about (40) credit reports per month.

Our access is primarily local; it may become regional and national at times.

You're Signature

Authorized Manager
XYZ Mortgage

To Expedite Your Approval, Please Be Sure to Return This Package Completed With The Following Documents

- ☐ A copy of your Mortgage Brokers, Bankers, Real Estate, or Applicable Business License.
- ☐ A copy of your lease reflecting your Company Name, Address, as well as the beginning and ending dates of the agreement
- ☐ A copy of an annual report published within the last (12) months
- ☐ A company email directory
- ☐ A copy of your firms listing in the telephone directory or business phone bill
- ☐ A copy of a pre-printed, voided company check
- ☐ A copy of the principles driver's license
- ☐ Completed Agreement w/ all fields filled out and signed
- ☐ Completed credit card authorization form for billing of registration fee
- ☐ Experian Pre-qual Questionnaire (If you would like the pre-qual product setup)
- ☐ A Letter of Intent on your company's letterhead, signed by an officer, owner, or authorized manager of the company. The Letter of Intent must include the following (see attached sample letter)
    - ✓ Must be on Company Letter head
    - ✓ The nature of your business
    - ✓ Your intended use for our services
    - ✓ Your anticipated monthly volume
    - ✓ Intent as to whether your access is anticipated to be primarily local, regional, or national.

***Note: An Onsite Physical Inspection is Required At Time of Approval**