SERVICE AGREEMENT

The firm listed above on the Service Application, hereinafter referred to as Client and/or End User, petitions UCS/TenantReports.com, hereinafter referred to as UCS/TenantReports.com, for the use of its services upon the basis outlined below. If accepted by UCS/TenantReports.com as a subscriber, Client agrees that the following shall constitute a service contract between Client and UCS/TenantReports.com.

1. The undersigned Client hereby petitions UCS/TenantReports.com to render service in accordance with applicable federal, state and local laws, rules regulations, orders and guidance from federal and state governmental agencies, including but not limited to, the Consumer Financial Protection Bureau and its customary practices. This Agreement states the terms and conditions under which UCS/TenantReports.com will provide consumer credit reports ("Reports") to Client for which Client agrees to promptly pay for all products and services ordered/requested by client.

These reports are based upon information obtained in good faith by one or more consumer reporting agencies (including Experian, Equifax, and TransUnion). UCS/TenantReports.com may from time to time increase the charges to Client by providing 60 days written notice to Client at its business address and in such event Client agrees to pay the revised charges unless Client terminates this Agreement as hereinafter provided.

2. Client agrees to make full payment within (30) calendar days after the date of each invoice from UCS/TenantReports.com.

3. If any litigation/arbitration between End User and UCS/TenantReports.com, whether relating to this Agreement or otherwise, in addition to all other appropriate relief the prevailing party will be entitled to recover its attorneys' fees and other costs incurred with the action.

4. Client hereby agrees, represents and warrants that it is the type of business listed in question 1 of the Service Application and in using the services of UCS/TenantReports.com, Client will, in all respects, comply with the provisions of 15 U.S.C. §1681 et seq. (Fair Credit Reporting Act, hereinafter referred to as FCRA) and that services will be requested only for the Client's exclusive use. Client further certifies that consumer reports will be ordered and used only in connection with a credit transaction involving the consumer 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.

5. Client certifies that it will request consumer reports pursuant to procedures that are prescribed by UCS / TenantReports.com from time to time and comply wi th appl icable law and only for the permissible purpose certified above, and will use the reports obtained for no other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with Client's own data, or otherwise in any service which is derived from the consumer reports.

Client shall use each consumer report only for a one-time use and shall hold the report in strict confidence, and not disclose or resell it to any third parties; provided however that (a) Client may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report, and (b) Client may disclose the report to any person if required to do so under Applicable Law. Moreover, for scores obtained from Trans Union, Equifax Information Systems, or Experian Information Solutions, Client shall not disclose to consumers or any third party, any or all such scores provided under this Agreement, except as required by Applicable Law which includes the use with a legitimate business purpose in connection with a business transaction that is initiated by the consumer. [Client agrees that consumer reports on employees will not be requested. Client will

maintain copies of all written authorizations for a minimum of 60 months from the date of inquiry.

Client further agrees, as requested, to promptly furnish, by telephone or in writing, to UCS/Tenant-Reports.com all required information covering transactions by the Client and its consumers, and to indemnify UCS/TenantReports.com, TransUnion, Equifax Information Services, Experian Information Solutions, any other consumer reporting vendors, and each of the other Clients and other officers and employees of each, jointly and severally, from any loss, damage, attorney's fees and costs arising from any claim or suit based on alleged violations of any provisions of this Agreement.

6. This Agreement shall continue in full force and effect without any fixed date of termination. Either party may terminate this Agreement upon providing ten (10) days written notice to the identified office of the other party. Client hereby acknowledges and understands that UCS/TenantReports.com shall not provide notice if any consumer reporting vendors direct UCS/TenantReports.com to halt delivery of any and all consumer reporting information. If UCS/TenantReports.com is directed to restrict Client's data privilege, it will be done immediately prior to notice.

Client has forty five (45) days to cure any violations, after notice by UCS/TenantReports.com. If any violation is not cured by client within this specified period of time, UCS/TenantReports.com, in its' sole discretion, has the option to terminate.

7. No information furnished to Client is guaranteed nor is UCS/TenantReports.com in any way responsible for such information. Absent negligence, misconduct, fraud or any breach of any covenant, obligation, duty, representation or warranty hereof, UCS/TenantReports.com shall not be responsible or liable for any loss caused by any of its servants, agents, attorneys, clerks or employees in procuring, collecting and communicating any information furnished by or to Client. No promise, statement, representation or agreement made by any employee or other representative of UCS/TenantReports.com and not expressed in this Agreement shall bind it contractually or otherwise to Client.

8. Client hereby agrees to comply with all policies and procedures required by UCS/TenantReports.com's consumer reporting vendors, Client may terminate this Agreement at any time after notification of a change in policy in the event Client deems such compliance is not within its best interest.

9. Client agrees that UCS/TenantReports.com and UCS/TenantReports.com's consumer reporting vendors shall have the right, upon written notice thereof, to audit records of Client that are relevant to the provision of services set forth in this Agreement during business hours on a business day.

Client further agrees that it will respond within a requested time frame for information requested by UCS/TenantReports.com's consumer reporting vendors regarding information provided by such vendor. Client understands that such vendor may suspend or terminate access to the vendor's information in the event Client does not cooperate with such an investigation.

10. (a) During the term of this Agreement, Client agrees to comply with all Applicable Law, including, the FCRA, with any changes enacted to the FCRA during the term of this Agreement, the Gramm Leach Bliley Act and its implementing regulations, any state or local laws governing the disclosure of consumer credit information, and any regulations or limitations promulgated by governmental agencies with respect to UCS/TenantReports.com's consumer reporting vendors. In addition, such new requirements might require price increases. Client agrees to comply with any such new requirements no later than thirty (30) days after it actually receives notice from UCS/TenantReports.com and such requirements shall be incorporated into this Agreement by this reference. Client understands and agrees that UCS/TenantReports.com may require evidence, including a certification that Client understands and will comply with applicable laws and regulations.

(b) Client will implement strict security procedures designed to ensure that Client's employees and customers use the services and the credit information in accordance with this Agreement and for no other purposes other than as permitted by this Agreement. Client will hold the services and the credit information in strict confidence and will restrict access to the services and the credit information to Client's employees and customers who agree to act in accordance with the terms of this Agreement and Applicable Law. Client will inform Client's employees and customers to whom any credit information is disclosed of the provisions of this Agreement. Client agrees to indemnify UCS/TenantReports.com for any losses incurred by UCS/TenantReports.com as a result of the misuse of the service or the credit information by Client or Client's affiliates, employees, agents, subcontractors or customers in violation of the Agreement.

11. (a) Client shall notify UCS/TenantReports.com of any breach of the security of consumer reporting data provided under this Agreement if the personal information of consumers was, or is reasonably believed to have been, acquired by an unauthorized person within 24 hours following discovery thereof. (b) In the event of such a breach, Client agrees to cooperate with UCS/TenantReports.com and with UCS/TenantReports.com's credit reporting vendors in any investigation relative thereto. The nature and timing of any notifications required herein shall be under the control of UCS/TenantReports.com's credit reporting vendors, unless otherwise required by Applicable Law.

(c) For purposes of this Agreement, "breach of the security of the system" means unauthorized acquisition of data that compromises

the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(d) For purposes of this Agreement, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number. (2) Driver's license number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(e) For purposes of this Agreement, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(f) For purposes of this Agreement, "notice" may be provided by one of the following methods:

(1) Written notice. (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC §7001. (3) E-mail notice, if Client agrees that email notice is acceptable if UCS/TenantReports.com utilizes the email information provided by Client on page (2) of the UCS/TenantReports.com Service Application.

(g) The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(h) The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law

enforcement agency determines that it will not compromise the investigation.

(i) In the event the breach is determined to be within the "Control of Client, as used herein refers to and means a determination by

UCS/TenantReports.com's credit reporting vendors, technical software vendors or other companies or professionals proficient in data security ("Security Experts") that the breach was a direct result of Client's actions or inactions to utilize appropriate safeguards which would have prevented the breach;

(1) Client shall provide to each affected or potentially affected consumer, credit history monitoring services for a minimum of one year in which the consumer's credit history is monitored and the consumer receives daily notification of the changes that may indicate fraud or ID theft from at least one of the national consumer credit reporting bureaus, and

(2) UCS/TenantReports.com may assess Client an expense recovery fee for additional charges and fees incurred as a result of the

breach.

12. If approved by UCS/TenantReports.com and UCS/TenantReports.com's consumer reporting vendors, Client may deliver the consumer credit information to a third party, secondary user with which Client has an ongoing business relationship for the permissible use of such information.

UCS/TenantReports.com's consumer reporting vendors may charge a fee for the subsequent delivery to secondary users.

13. Client agrees that UCS/TenantReports.com may verify, through audit or otherwise, that Client is in fact the end user of the credit information with no intention to resell or otherwise provide or transfer the credit information in whole or in part to any other person or entity.

14. Client agrees to notify UCS/TenantReports.com of any change or ownership or control prior to any such change. UCS/TenantReports.com may require the new ownership to re-apply for the services provided for herein and may require a new physical inspection in the event the office location is changed.

15. Client hereby authorizes UCS/TenantReports.com to provide information regarding Client to UCS/TenantReports.com's Consumer reporting vendors. UCS/TenantReports.com agrees to notify Client if any consumer reporting vendors make an inquiry regarding Client.

16. Client agrees that UCS/TenantReports.com may monitor Client on an ongoing basis to determine Client's compliance with Applicable Law and the provisions of this Agreement. In the event UCS/TenantReports.com determines that Client is not in compliance with Applicable Law or this Agreement, UCS/TenantReports.com may immediately discontinue services to the Client under this Agreement. Client shall remain responsible for the payment for any services provided to Client by UCS/TenantReports.com prior to any such discontinuance.

17. Client agrees that it is their sole responsibility to be familiar with all applicable laws and regulations regarding this Agreement. Client agrees to comply with all applicable laws and regulations, including but not limited to, the FCRA and the policies and procedures required by UCS/TenantReports.com's consumer reporting vendors. UCS/TenantReports.com has provided the attached Appendices for general knowledge; however, Client agrees that it is their sole responsibility to be cognizant of any and all laws or regulations pertaining to this Agreement and it is the Clients sole responsibility to train their employees, agents and subcontractors accordingly.

18. OFAC Alert is a service that is based on data that was not collected, in whole or in part, for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes; or any other purpose authorized under the FCRA. Accordingly, Client certifies it will not use any information provided through the OFAC Alert Service as part of its decision-making process for determining the consumer's eligibility for any credit products or other products, benefits (including the opportunity to rent a dwelling or services applied for. Client acknowledges that such an indicator is merely a message that the consumer may be listed on one or more U.S. Government maintained lists of persons subject to economic sanctions, and Client further certifies that upon receipt of an OFAC Alert, it will contact the

appropriate government agency for confirmation and instructions. The OFAC Alert indicator may or may not apply to the consumer whose eligibility is being considered by Client.

19. Client acknowledges additional responsibility and guidelines regarding credit scores provided by UCS/TenantReports.com, attached to this Agreement as Appendix A and agrees to be compliant with the responsibility outlined in Appendix E.

20. UCS/TenantReports.com offers a program to facilitate the revision of data contained in consumer credit files, in an expedient manner, thereby adjusting scores of those consumers. If Client utilizes this service, known as "Rapid ReScore," Client acknowledges adherence to additional responsibilities and guidelines.

21. Client agrees to fully support and implement policies that protect the confidential nature of information furnished by and through

UCS/TenantReports.com and insure respect for consumers' rights to privacy. Client will subscribe to the Access Security Requirements furnished on Appendix C and will make all employees who access credit aware of these policies.

22. California Law Certification. Client will refer to Appendix E in making that certification and Client agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act. To the extent any provisions of the California Civil Code applies to any report requested by Client, Client agrees that they will be responsible for full compliance with all requirements of the California Civil Code, and that UCS/TenantReports.com will have no such responsibility.

23. 15 U.S.C. §1681 et seq. of the FCRA also requires certain other responsibilities of users of consumer reports from consumer reporting agencies. Those responsibilities are attached (and made a part hereof) as Appendix B to this Agreement. Furthermore, Client acknowledges their responsibilities under the FCRA and agrees to comply with all requirements.

24. Vermont Certification. Client will refer to Appendix F in making that certification and Client agrees to comply with all applicable provisions under Vermont Law.

25. Client acknowledges that many services provided also contain information from the Death Master File as issued by the Social Security Administration ("DMF"); certify pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. §1110.102 that, consistent with its applicable FCRA or GLB use of information, the client's use of deceased flags or other indicia within the information is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. §1110.102(a)(1); and certi-

fy that the client will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the information.

26. Client acknowledges that it does not engage in any of the business areas outlined in Appendix G to this Agreement.

27. Client agrees to fully support and implement policies that enables it compliance with UCS/Tenant-Reports.com's Internet Security Requirements as outlined in Appendix H to this Agreement

28. 15 U.S.C. §1681 ET SEQ. PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CREDIT REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, UNITED STATES CODE, IMPRISONED FOR NOT MORE THAN TWO YEARS, OR BOTH.

29. This Agreement sets forth the parties' entire understanding with respect to the subject matter here-of and shall be governed by and construed under the laws of the Commonwealth of Pennsylvania.

.

DATED this day of , 20

AUTHORIZATION AND ACCEPTANCE UCS/TenantReports.com

CLIENT NAME BY (PRINT)

BY (PRINT) SIGNATURE

SIGNATURE TITLE

DATE DATE

APPENDIX A

CREDIT RISK SCORE ADDENDUM TO USER SERVICE AGREEMENT

UCS/TenantReports.com warrants that it has an Agreement for service and an account in good stand-ing with Client for a permissible purpose under the Fair Credit Reporting Act to obtain the information in a Fair Isaac Credit Repository Score(s) (FICO Classic, FICO, Beacon) and their reason codes generated by Experian, TransUnion, Equifax.

Client agrees to maintain internal procedures to minimize the risk of unauthorized disclosure and cer-tifies that all scores and rea son codes whether oral or written shall be maintained in strict confidence and disclosed only to employees whose duties 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 hereunder, except as otherwise required by law.

Notwithstanding any contrary provision of this Agreement, Client may disclose the Scores provided to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only.

Unless explicitly authorized in this Agreement or in a separate Agreement between Client and UCS/TenantReports.com for scores obtained from credit repository, or as explicitly otherwise authorized in

advance and in writing by credit repository through UCS/TenantReports.com, Client shall not disclose to consumers or any third party, any or all such scores provided under this Agreement, unless required by law.

Reason codes may be utilized to assist in preparing an adverse action (denial letter) to consumer. Client shall comply with all applicable law in using the Scores and reason codes. Client, its employees, agents or subcontractors may not use the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of the credit repositories, Fair Isaac and Company, UCS/TenantReports.com, the affiliates of them or of any other party involved in the provisions of the Score without such entity's prior written consent.

Client agrees, either directly or indirectly not in any matter whatsoever, to discover or reverse engineer any confidential and proprietary criteria developed or used by Credit Repository/Fair Isaac in performing the Credit Repository Score.

Warranty: Credit Repository/Fair Isaac warrants the Credit Repository Score Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Credit Repository Score Model is applied is similar to the population sample on which the Credit Repository Score Model was developed. Credit Repository Score Model may be relied upon by UCS/TenantReports.com and/or Client to rank consumers in order of the risk of unsatisfactory payment such consumers might present to Broker. Credit Repository/Fair Isaac further warrants that so long as it provides the Credit Repository Score Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC §1692 et seq.

THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES FICO HAS GIVEN UNIVERSAL CREDIT SERVICES AND/OR CLIENT WITH RESPECT TO THE FAIR ISAAC MODEL, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, FICO MIGHT HAVE GIVEN UNIVERSAL CREDIT SERVICES AND/OR CLIENT WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR F1TENSS FOR A PARTICULAR PURPOSE.

UCS/TenantReports.com's and Client's rights under the foregoing warranty are expressly conditioned upon each respective applicant's periodic revalidation of the Credit Repository Score Model in compliance with the requirements of regulation B as it may be amended from time to time (12 CFR 202 et seq.)

Client agrees to limit the aggregate liability of Experian/Fair 12 CFR of 202, et seq. Isaac to the lesser of the fees paid by the Client for Experian/Fair Isaac Model sold to Client during the six (6) month period immediately preceding Client's claim and excluded any liability of Experian/Fair Isaac for incidental, indirect, special or consequential damages of any kind.

CLASSICSM CREDIT RISK SCORE SERVICES

(TransUnion's Required Terms for Addendum to Subscriber Agreement for Consumer Reports between Reseller and its Customer)

1. Based on an agreement with TransUnion LLC ("TransUnion") and Fair Isaac Corporation ("Fair Isaac") ("Reseller Agreement"), Reseller has access to a unique and proprietary statistical credit scoring service jointly offered by TransUnion and Fair Isaac which evaluates certain information in the credit reports of individual consumers from TransUnion's data base ("Classic") 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 "Classic Score").

2. Subscriber, from time to time, may desire to obtain Classic Scores from Trans Union via an on-line mode in connection with consumer credit reports.

3. Subscriber has previously represented and now, again represents that it is a tenant screening company and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").

4. Subscriber certifies that it will request Classic Scores pursuant to procedures prescribed by Reseller from time to time only for the permissible purpose certified above, and will use the Classic Scores obtained for no other purpose.

5. Subscriber will maintain copies of all written authorizations for a minimum of three (3) years from the date of inquiry.

6. Subscriber agrees that it shall use each Classic Score only for a one-time use and only in accordance with its permissible purpose under the FCRA.

7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, Reseller may, upon its election, discontinue serving the Subscriber and cancel this Agreement, in whole or in part (e.g., the services provided under this Addendum only) immediately.

8. Subscriber recognizes that factors other than the Classic 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. Trans Union 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 Subscriber with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg. B"). However, the Classic Score itself is proprietary to Fair Isaac, 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: (1) 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; or (2) as clearly required by law.

Subscriber will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and Trans Union's prior written consent

11. In the event Subscriber intends to provide Classic Scores to any agent, Subscriber may do so provided, however, that Subscriber first enters into a written agreement with such agent that is consistent with Subscriber's obligations under this Agreement. Moreover, such agreement between Subscriber and such agent shall contain the following obligations and acknowledgments of the agent: (1) Such agent shall utilize the Classic Scores for the sole benefit of Subscriber and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit; (2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party

without TransUnion and Fair Isaac's prior written consent 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; or (b) as clearly required by law;

(3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration; (4) Such agent shall not resell the Classic Scores; and (5) Such agent shall not use the Classic Scores to create or maintain a database for itself or otherwise.

12. Subscriber acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information will result in an inquiry being added to the consumer's credit file.

13. Subscriber shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject.

14. The information including, without limitation, the consumer credit data, used in providing Classic 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 involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed. Moreover, in no event shall TransUnion, Fair Isaac, nor their officers, employees, affiliated companies or bureaus, independent contractors or agents be liable to Subscriber for any claim, injury or damage suffered directly or indirectly by Subscriber as a result of the inaccuracy or incompleteness of such information used in providing Classic Scores under this Agreement and/or as a result of Subscriber's use of Classic Scores and/or any other information or serviced provided under this Agreement.

15.1 Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to TransUnion and used in the computation of the Classic Score ("Models") are empirically derived from TransUnion's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that 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 used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and Regulation B promulgated there under. Classic provides a statistical evaluation of certain information in TransUnion's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring relative to other individuals in TransUnion's database. 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.

15.2 THE WARRANTIES SET FORTH IN SECTION 15.1 ARE THE SOLEWARRANTIES MADE UNDER THIS ADDENDUM

CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANSUNION 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 INSECTION 15.1 ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

16. 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 NOTWITHSTANDINGANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

17. THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO SUBSCRIBER, IN NO EVENT SHALL THE AFORE STATED 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 THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM SUBSCRIBER'S BREACH, DIRECTLY OR THROUGH SUBSCRIBER'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT.

18. ADDITIONALLY, NO PARTY 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 ACCRUED. IN NO EVENT SHALL ANY PARTY'S TOTAL LIABILITY, IF ANY,UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY SUBSCRIBER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS ($10,000.00) WHICHEVER AMOUNT IS LESS.

19. This Addendum may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this Addendum by Subscriber; (2) in the event the agreement(s) related to Classic between TransUnion, Fair Isaac and Reseller are terminated or expire; (in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation by any governmental entity.

APPENDIX B

NOTICE TO USERS OF CONSUMER REPORTS AND OBLIGATIONS UNDER FCRA

The Fair Credit Reporting Act (FCRA), 15 USC §1681-1681Y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Federal Trade Commission's Website at http://www.ftc.gov/credit. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Commission's Web site. Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are as follows:

• As ordered by a court or a federal grand jury subpoena, see Section 604 (a)(I)

• As instructed by the consumer in writing, see Section 604 (a)(2)

• For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account, see

Section 604(a)(3)(A)

• For employment purposes, including hiring and promotion decisions, where the consumer has given written permission, see Sections 604(a)(3)(B) and 604(b)

• For the underwriting of insurance as a result of an application from a consumer, see Section 604(a)(3)(C)

• When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer, see Section

604(a)(3)(F)(i)

• To review a consumer's account to determine whether the consumer continues to meet the terms of the account, see Section

604(a)(3)(F)(ii)

• To determine a consumer's eligibility for a license or other benefit granted by a governmental entity required by law to

consider an applicant's financial responsibility or status, see Section 604(a)(3)(D)

• For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks

associated with an existing credit obligation, see Section 604(a)(3)(E)

• For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof, see Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(a) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term “adverse action” is defined very broadly by Section 603. “Adverse actions” include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA — such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following

• The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that

provided the report.

• A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.

• A statement setting forth the consumer’s right to obtain a free disclosure of the consumer’s file from the CRA if the consumer makes a request within 60 days.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon

information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section

615(b)(l) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer’s written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 6l5(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If the consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(b) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed, which will be issued by the Federal Trade Commission and the banking and credit union regulators. The Federal Trade Commission's regulations are available at http://www.ftc.gov/credit.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The Federal Trade Commission, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Federal Trade Commission's regulations may be found at http://www.ftc.gov/credit.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations to be jointly prescribed by the Federal Trade Commission and the Federal Reserve Board.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home loan Applicant").

III. OBLIGATIONS OF USERSWHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

• Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely

of the disclosure, that a consumer report may be obtained.

• Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.

• Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any

federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a

copy of the report and a summary of the consumer's rights will be provided to the consumer.

• Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken. An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2) outlines the procedures for investigative consumer reports and employee misconduct investigations are set forth below.

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONSWHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subject of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

• The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written

disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on

which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request

additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)

• The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure

described below.

• Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 613(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its company complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes — or in connection with a credit transaction (except as provided in regulations issued by the banking and credit union regulators) — the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or

insurance under certain circumstances. See Sections 603(I)604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (I) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

• Information contained in a consumer's CRA file was used in connection with the transaction.

• The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the

offer.

• Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the

criteria used for screening or any applicable criteria on credit worthiness or insurability, or the consumer does not furnish required

collateral.

• The consumer may prohibit the use of information in his or her file in connection with future pre-screened offers of credit or

insurance by contacting the notification system established by the CRA that provided the report. The statement must include the

address and toll-free telephone number of the appropriate notification system.

In addition, once the Federal Trade Commission by rule has established the format, type size, and manner of the disclosure required by Section 615(d), users must be in compliance with the rule. The FTC's regulations will be at http://www.ftc.gov/credit.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

Disclose the identity of the end-user to the source CRA.

Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to

obtain:

1. the identity of all end-users;

2. certifications from all users of each purpose for which reports will be used; and

3. certification that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must

make reasonable efforts to verify this information before selling the report.

B. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCPA can result in state government or federal government enforcement actions, as well as private lawsuits. See Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. See Section 619.

The FTC's Web site, http://www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA. Citations for FCRA sections in the U.S. Code, 15 U.S.C. ~ 1681 et seq.:

Section 602 15 U.S.C. 1681 Section 615 15 U.S.C. 1681m

Section 60315 U.S.C. 1681a Section 616 15 U.S.C. 1681n

Section 604 15 U.S.C. 1681b Section 617 15 U.S.C. 1681o

Section 605 15 U.S.C. 1681c Section 618 15 U.S.C. 1681p

Section 605A 15 U.S.C. 1681cA Section 619 15 U.S.C. 1681g

Section 605B 15 U.S.C. 1681cB Section 620 15 U.S.C. 1681r

Section 606 15 U.S.C. 1681d Section 621 15 U.S.C. 1681s

Section 607 15 U.S.C. 1681e Section 622 15 U.S.C. 1681s-1

Section 608 15 U.S.C. 1681f Section 623 15 U.S.C. 1681s-2

Section 609 15 U.S.C. 1681g Section 624 15 U.S.C. 1681t

Section 610 15 U.S.C. 1681h Section 625 15 U.S.C. 1681u

Section 611 15 U.S.C. 1681i Section 626 15 U.S.C. 1681v

Section 612 15 U.S.C. 1681j Section 627 15 U.S.C. 1681w

Section 613 15 U.S.C. 1681k Section 628 15 U.S.C. 1681x

Section 61415 U.S.C. 16811 Section 629 15 U.S.C. 1681y

APPENDIX C

ACCESS SECURITY REQUIREMENTS

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. The credit reporting agency reserves the right to make changes to Access Security Requirements without notification. This information provides minimum baselines for information security.

In accessing the credit reporting agency's services, you agree to follow these security requirements:

1. Implement Strong Access Control Measures

1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.

1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.

1.3 You must request your Subscriber Code password be changed immediately when:

• any system access software is replaced by system access software or is no longer used;

• the hardware on which the software resides is upgraded, changed or disposed of

1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information.

Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).

1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit

reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.

1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.

1.7 Keep user passwords Confidential. Ensure that passwords are not transmitted, displayed or stored in clear text. Protect all end user passwords using encryption or a cryptographic hashing algorithm. When using encryption, ensure that strong encryption algorithms are utilized (e.g. AES 256 or above)

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) alpha/numeric characters for standard user accounts

1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.

1.10 Active logins to credit information systems must be configured with a 30 minute timeout for inactive sessions.

1.11 Restrict the number of key personnel who have access to credit information.

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 your membership application.

1.13 Ensure that you and your employees do not access your 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.

1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency 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.

1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.

1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit

information.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s) i.e., firewalls, routers, servers, personal computers (laptop and desktop) and all other systems current

with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, 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 computer virus detection/scanning product on all computers,

systems and networks. Anti-virus software deployed must be capable to detect, remove and protect against all known types

of malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.

• If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until

the virus has been eliminated.

• On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and

installing new virus definition files.

2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:

• Use, implement and maintain a current, commercially available computer anti-Spyware product on all computers, systems

and networks.

• If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until

the problem has been resolved and eliminated.

• Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your

computers.

• Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware

definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which

prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more

frequently than weekly.

3. Protect Data

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 All credit reporting agency data is classified as confidential and must be secured to this requirement 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 credit reporting agency data and information when stored on any laptop computer and in the database using AES or

3DES with 128-bit key encryption at a minimum.

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

3.6 Data obtained from the credit reporting agency must NOT be stored locally on tablets or smart phones.

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

3.8 Applications utilized to access data via tablet or smart phones must protect data while in transmission using SSL protection and/or use of VPN or equivalent.

4. Maintain an Information Security Policy

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

4.2 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.

4.3 The FACTA Disposal Rules requires that you 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.

4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to emphasize the importance of security within your organization.

5. Build and Maintain a Secure Network

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 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.

5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the

configuration of the access point.

5.7 When using service providers (e.g. software providers) to access data, access to third party tools/ services must require

multi-factor authentication.

6. RegularlyMonitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).

6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency 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 credit reporting agency data on mobile devices is prohibited. Any exceptions must be obtained from UCS/TenantReports.com

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 credit reporting agency 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 credit reporting agency 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 credit reporting agency 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 – PCS DSS – EI3PA

 SSAE 16 – SOC2 or SOC3

 FISMA

 CAI / CCM assessment

8. General

8.1 UCS/TenantReports.com may from time to time audit the security mechanisms Company maintains to safeguard access to credit reporting agency 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 credit reporting agency information and systems via third party software, the Company agrees to make available to UCS/TenantReports.com 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 credit reporting agency 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 credit reporting agency information systems; this applies to both in-house and 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 servers/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 credit reporting agency systems shall be made available to

UCS/TenantReports.com upon request, for example during breach investigation or while performing audits.

8.6 Data requests from Company must include the IP address of the device from which the request originated, where applicable.

8.7 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 credit reporting agency services, systems or data and (d) will abide by the provisions of these requirements when accessing credit reporting agency data.

8.8 Company understands that its use of Experian networking and computing resources may be monitored and audited by Experian,

without further notice.

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

8.10 When using third party service providers to access, transmit, or store credit reporting agency data, additional documentation may be required by UCS/TenantReports.com.

Record Retention: The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, the credit reporting agency 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 breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency 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."

APPENDIX D

INTERNET DELIVERY SECURITY REQUIREMENTS

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with

UCS/TenantReports.com on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to UCS/TenantReports.com 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 UCS/TenantReports.com product based upon the legitimate business needs of each employee. UCS/TenantReports.com 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 UCS/TenantReports.com. 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). UCS/TenantReports.com approval of requests for (Internet) access may be granted or withheld in its sole discretion. UCS/TenantReports.com 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 UCS/TenantReports.com 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 UCS/TenantReports.com 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 UCS/TenantReports.com on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users. 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 UCS/TenantReports.com sys-

tems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to UCS/TenantReports.com immediately.

2. As a Client to UCS/TenantReports.com 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 UCS/TenantReports.com 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 UCS/TenantReports.com Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding UCS/TenantReports.com 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 UCS/TenantReports.com 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 UCS/TenantReports.com regarding access to UCS/TenantReports.com products and services.

7. Shall immediately report changes in their Head Security Designates status (e.g. transfer or termination) to UCS/TenantReports.com.

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 UCS/TenantReports.com when needed on any system or user related matters.

APPENDIX E

END USER CERTIFICATION OF COMPLIANCE California Civil Code §1785.14(a)

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

Section 1785.14(a)(l) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address listed on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, ("End User") hereby certifies to Consumer Reporting Agency that End User IS NOT a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person. End User also certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

APPENDIX F

VERMONT FAIR CREDIT REPORTING STATUTE, 9 V.S.A §2480E (1999)

§2480e. Consumer consent

(a) A person shall not obtain the credit report of a consumer unless:

(1) the report is obtained in response to the order of a court having jurisdiction to issue such an order; or

(2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer

(b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.

(c) Nothing in this section shall be construed to affect:

(1) the ability of a person who has secured the consent of the consumer pursuant to subdivision (a)(2) of this section to include in his or her request to the consumer, permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and (2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade

Commission.

VERMONT RULES *** CURRENT THROUGH JUNE 1999 ***

AGENCY 06. OFFICE OF THE ATTORNEY GENERAL

SUB-AGENCY 031. CONSUMER PROTECTION DIVISION

CHAPTER 012. Consumer Fraud — Fair Credit Reporting

RULE CF 112 FAIR CREDIT REPORTING

CVR 06-031-012, CF 112.03 (1999)

CF 112.03 CONSUMER CONSENT

(d) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental benefit in a manner other than in writing, then the person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request. The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

(e) Consumer consent required pursuant to 9 V.S.A. §§ 2480e and 2480g shall be deemed to have been obtained in writing if, after a clear and adequate written disclosure of the circumstances under which a credit report or credit reports may be obtained and the purposes for which the credit report or credit reports may be obtained, the consumer indicates his or her consent by providing his or her signature.

(c) The fact that a clear and adequate written consent form is signed by the consumer after the consumer's report has been obtained pursuant to some other form of consent shall not affect the validity of the consent.

APPENDIX G

PROHIBITED BUSINESSES AND INDUSTRIES

ENTITIES THAT CANNOT BE PROVIDED INFORMATION

Adult entertainment services of any kind

A business that operates out of an apartment or unrestricted location within a residence.

Attorneys or Law offices, except Bankruptcy Attorneys for bankruptcy filing purposes.

Bail Bondsman

Check cashing establishment

Credit counseling (unless 501c3)

Credit repair clinic

Dating Service

Financial counseling

Genealogical or heir research firm

Massage Services

Company that locates missing children

Pawn shop

Private Detectives, detective agencies or investigative companies

Individual seeking information for their private use

Company that handles third-party repossession

Company or individual involved in spiritual counseling

Subscriptions (magazines, book clubs, record clubs, etc.)

Tattoo service

Insurance claims

Internet locator services

Asset location services

Future services (i.e., health clubs, timeshare, continuity clubs, etc.)

News agencies or journalists

Law enforcement (except for employment screening purposes)

Any company or individual who is known to have been involved in credit fraud or other unethical business practices

Companies listed on repository alert report notifications

APPENDIX H

REQUIRED INTERNET SECURITY PROCEDURES

Client is required to implement the following security procedures ("Procedures") required to order and receive Credit Reports through the UCS/TenantReports.com Website. Failure of Client to follow any of the Procedures may lead to a suspension or termination of Client's ability to order and receive Credit Reports through the UCS/TenantReports.com Website.

1. To order and receive Credit Reports through the TenantReports.com Website, Client must use the subscriber number and password assigned to Client by UCS/TenantReports.com (together, "UCS/TenantReports.com Password"). Orders for Credit Reports must include the name, social security number, and address of the subject of the Credit Report, and any other information specified by UCS/TenantReports.com. The operator must have a UCS/TenantReports.com unique UCS/TenantReports.com Website identification and password. Sharing the identification and password is strictly prohibited. All Credit Reports delivered by UCS/TenantReports.com to Client through the TenantReports.com Website will be encrypted. Client must use an internet browser that supports 128-bit encryption.

2. Client must protect the UCS/TenantReports.com Password so that only authorized employees of Client ("Authorized Employees") have access to this information. Client agrees to limit Authorized Employees to those employees who have a need to know the UCS/TenantReports.com Password to carry out their official duties with Client. Client will not post the UCS/TenantReports.com Password at its facilities, and Client will take all other actions necessary to prevent unauthorized persons from gaining knowledge of the UCS/TenantReports.com password. The UCS/TenantReports.com Password must not be released by telephone to any telephone caller, even if the caller claims to be a UCS employee. UCS/TenantReports.com reserves the right to change the UCS/TenantReports.com Password at any time to prevent unauthorized access to Credit Reports delivered to Client through the UCS/TenantReports.com Website.

3. All access software used by Client to order and obtain Credit Reports through the UCS/TenantReports.com Website, whether developed by Client or purchased from a third-party vendor must have the UCS/TenantReports.com Password "hidden" or embedded so that the UCS/TenantReports.com Password is known only to Authorized Employees. Each Authorized Employee must be assigned a unique logon code ("Logon Code") to be able to open and use the TenantReports.com Website. Authorized Employees will be required to protect the secrecy of their Logon Codes, and as soon as an Au-

thorized Employee loses such status (whether by termination of employment or otherwise), Client will immediately disable such employee's Logon Code. Logon Codes will be changed at least once every 90 days.

4. Prior to providing an Authorized Employee with access to the CCL Password, Client will provide the Authorized Employee with adequate training regarding the requirements of these Procedures and applicable laws, and will require the Authorized Employee to agree to comply with all the requirements set forth below ("Employee Requirements"). Client agrees not to add any employee as an Authorized Employee unless the employee receives the required training. All Authorized Employees must comply with the following Employee Requirements:

(a) The employee must have read these Procedures and the Agreement for Service and be familiar with the requirements as to the

permissible purposes for which Credit Reports may be ordered from UCS/TenantReports.com and the restrictions on the use and

dissemination of such reports and the information therein, and must agree to comply with such requirements and restrictions.

(b) The employee must agree not to disclose the UCS/TenantReports.com Password or the Logon Code assigned to the employee to any other person.

(c) The employee must agree not to order Credit Reports from UCS/TenantReports.com except in performance of the employee's

official duties for Client. The employee must acknowledge his or her awareness that the Fair Credit Reporting Act provides that "any

person who knowingly and willfully obtains information on a consumer from a consumer reporting agency [such as

UCS/TenantReports.com] under false pretenses shall be fined under Title 18 United States Code, imprisoned for not more

Than 2 years, or both."

(d) The employee must acknowledge that Credit Reports contain extremely sensitive information, and agree to protect the privacy of

such information by using Credit Reports obtained from UCS/TenantReports.com solely in connection with the employee's official

duties for Client, nor copying such Credit Reports (except as required by the employee's official duties), not providing such Credit

Reports or any information therein to any person (except in the course of the employee's official duties), and taking adequate

steps to prevent unauthorized persons gaining access to such reports or information.

(e) The employee must agree that after termination of his or her employment by Client or Client's with-

drawal of the employee's

designation as an Authorized Employee, the employee will not obtain or attempt to obtain Credit Reports from

UCS/TenantReports.com through the UCS/TenantReports.com Password or the employee's Logon Code for any reason.

5. Client will also follow UCS/TenantReports.com's general Access Security Procedures and agrees to establish such additional security procedures as may be specified by UCS/TenantReports.com from time to time.

APPENDIX J

Death Master File

End User certifies that it meets the qualifications of a Certified Person under 15 CFR § 1110 and that its access to the DMF is appropriate because:

1. End User has a legitimate fraud prevention interest, or has a legitimate purpose pursuant to a law, governmental rule, regulation or fiduciary duty, and shall specify the purpose for so certifying: and

2. End User has systems, facilities, and procedures in place to safeguard the accessed information; experience in maintaining the confidentiality, security, and

appropriate us e of the accessed information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986; and agrees to satisfy the requirements of such section 6103 (p)(4) if such section applies to End User; and

3. End User shall not disclose information derived from the DMF to the consumer or any third party, unless clearly required by law.

End User acknowledges that failure to comply with the provisions of 15 CFR § 1110 may result in penalties, among other items, of $1000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year. End User shall indemnify and hold harmless UCS/TenantReports.com, its reporting providers, and the US Government/NTIS from all claims, demands, damages,

expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with End User's, or End User's employees, contractors, or subcontractors, use of the DMF. This provision shall survive termination of the service agreement and will include any and all claims or liabilities arising from intellectual property rights.

Neither UCS/TenantReports.com, its reporting providers, nor the US Government/NTIS (a) make any warranty, express or implied, with respect to information provided under this section of the policy, including, but not limited to, implied warranties of merchantability and fitness for any particular use: (b) assume any liability for any direct, indirect or consequential damages incurred from any use of any part of the DMF, including infringement of third party intellectual property rights; and (c) assume any liability for any errors or omissions in the DMF.

End User is aware that the DMF does have inaccuracies and neither NTIS nor the Social Security Administration (SSA), which provides the DMF to NTIS, guarantee the accuracy of the DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the DMF is

not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the DMF.

End User acknowledges that any individual who claims that the SSA has incorrectly listed someone as deceased, or has incorrect dates/data pertaining to an individual on the DMF, will be directed to contact their local SSA office with proof to have the error corrected.