For ACRAnet Use Only
Company Name: _____

Client #: _____

CLIENT SERVICE AGREEMENT
Bankruptcy Attorney
("Agreement")

This Agreement is made as of the date indicated below by and between

_____

the undersigned (hereinafter referred to as "Client") and ACRAnet, Inc a Nevada Corporation (hereinafter referred to as "ACRAnet").

I. Client desires to receive consumer reports, credit worthiness scores, and other information (each and all of such reports, credit worthiness scores and other information being hereinafter included within the term "Consumer Reports") from ACRAnet. Client agrees that the Consumer Reports will be ordered and used by Client, subject to the terms and conditions of this Agreement and applicable law.

II. Client represents, warrants and covenants to ACRAnet that:

A. Client is not a private detective, media, news agency or journalist, detective agency, investigative company, bail bondsman, attorney, law enforcement, dating service, asset location service, future services, adult entertainment of any kind, check cashing service, massage service, pawn shop, tattoo service, credit or financial counseling firm, "credit repair clinic," internet locator service, diet center, adoption search firm, or a person that will not be an end-user of the Consumer Reports. Client will notify ACRAnet immediately if any of the foregoing changes.

B. Client certifies that Client will order Consumer Reports solely for one of the following purposes (Client agrees that other permissible purposes, such as employment screening, may require additional agreements) and for no other purpose: **initial only the following which apply.**

Initial here _____ In connection with the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 at the written request of the consumer on whom the information is to be furnished.

Client will order Consumer Reports only for Client's exclusive use, hold the Consumer Reports in strict confidence, and will not resell or otherwise disclose Consumer Reports (or any part thereof), except to the consumer or if adverse action has been taken based on the Consumer Report and/or is otherwise required by law. Client will (1) verify the identity of each consumer who is the subject of the Consumer Reports; (2) refer consumers to ACRAnet for all substantive inquiries regarding the Consumer Reports; (3) permit ACRAnet to audit, during business hours and without prior notice, Client's use of Consumer Reports, procedures and to assure compliance with this agreement and the Fair Credit Reporting Act. Client will not transmit any Consumer Report through the Internet without ACRAnet's prior written consent; and (4) Client will retain permissible purpose documentation for a minimum of five years after date of access.

III. The Fair Credit Reporting Act ("FCRA") provides that any person **"who knowingly and willfully obtains information on a consumer from a consumer reporting agency (such as ACRAnet) under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two years, or both."** Client acknowledges that ACRAnet has provided Client a copy of the CFPB's "Notice to Users of Consumer Reports: Obligations of Users under the FCRA," attached hereto, marked **Attachment "A"**. Client agrees to comply with all requirements of the FCRA, GLB, and other applicable laws in ordering and using Consumer Reports.

IV. A. Client shall indemnify, defend, and hold ACRAnet, its agents and its data resources including, but not limited to, Equifax, Trans Union and Experian and their respective agents, employees and independent contractors (herein collectively referred to as "Data Providers") harmless from and against any damages, losses, obligations, liabilities, claims, actions or causes of action (each and all of such items being hereinafter separately and collectively referred to as the "Claim") sustained or suffered by ACRAnet arising out of or relating to:

(1) Any breach of any representation, warranty, covenant or agreement made by Client in this Agreement, or in any certificate, instrument or agreement delivered by Client pursuant hereto or thereto or in connection with the transactions contemplated hereby or thereby or any facts or circumstances constituting such breach

(2) Any Claim by any consumer or any other third party, except to the extent directly caused by ACRAnet's gross negligence.

(3) Any Claim sustained or suffered by ACRAnet arising out of or relating to Client's execution, delivery or performance of this Agreement.

(4) All reasonable costs and expenses (including, without limitation, reasonable attorneys', accountants' and other professional fees and expenses) incurred by them in connection with any action, suit, proceeding, demand, assessment or judgment incident to any of the matters indemnified against under subparagraphs (1), (2) and (3) immediately above.

(5) Any Claim resulting from the publishing or other disclosure of the Consumer Report and/or credit scores.

B. ACRAnet shall give written notice to Client of any assertion of liability by a third party which might give rise to a Claim

by ACRAnet against the Client based on the indemnity contained herein, stating the nature and basis of said assertion and the amount thereof, to the extent known.

C. The defense of any suit, action, legal proceeding or administrative proceeding (each and all of such suits, actions, legal proceedings and/or administrative proceedings being hereinafter referred to as the "Proceeding") that may be threatened, brought or instituted against ACRAnet on account of any matter which is or may be the subject of the indemnity provided for herein shall be conducted at the sole expense of Client by legal counsel unilaterally selected by ACRAnet.

D. ACRAnet shall be kept fully informed by Client at all stages of the Proceeding. Client shall not make any settlement in or with respect to any Proceeding without the prior written consent of ACRAnet. Nothing contained herein shall mean or be construed to mean that ACRAnet shall not have the right to participate in the Proceeding represented by legal counsel unilaterally selected by ACRAnet.

E. If Client does not assume the defense of any such Claim or litigation resulting there from, ACRAnet may defend against such Claim or litigation, after giving notice of the same to Client, on such terms as ACRAnet may deem appropriate, and Client shall be entitled to participate in (but not control) the defense of such action, with Client's legal counsel and at Client's own expense. If Client thereafter seeks to question the manner in which ACRAnet defended such Claim or the amount or nature of any such settlement, Client shall have the burden to prove by a preponderance of the evidence that ACRAnet did not defend or settle such Claim in a reasonably prudent manner.

F. The remedies provided for in this Section shall be cumulative and shall not preclude assertion by ACRAnet of any other rights or the seeking of any other remedies against Client.

G. Client acknowledges ACRAnet's Access Security Requirements, attached hereto, and incorporated herein by reference. Client agrees to comply with all such requirements, as may be modified by ACRAnet from time to time, and to give all employees, agents and subcontractors of Client a copy prior to providing them authority to order, or any other access to, Consumer Reports. Client agrees to take all necessary measures to prevent unauthorized access to information through ACRAnet. Client will keep access codes strictly confidential and will establish and enforce policies allowing access to information only as permitted by State and Federal Regulation including Washington State Fair Credit Reporting Act (RCW 19.182.005, et seq) or Federal Fair Credit Reporting Act 15 U.S.C. 168(b) et seq. ("FCRA").

V. The accuracy, completeness, and validity of Consumer Reports are not guaranteed by ACRAnet and its agents, and all Consumer Reports are provided "AS IS." **ACRANET AND ITS AGENTS MAKE NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND IMPLIED WARRANTIES ARISING FROM A COURSE OF DEALING OR A COURSE OF PERFORMANCE, WITH RESPECT TO CONSUMER REPORTS INCLUDING, WITHOUT LIMITATION, WITH RESPECT TO THE ACCURACY, VALIDITY, OR COMPLETENESS OF ANY CONSUMER REPORT, THAT SUCH CONSUMER REPORT WILL MEET CLIENT'S NEEDS, OR THAT SUCH CONSUMER REPORT WILL BE PROVIDED ON AN UNINTERRUPTED BASIS, AND ACRANET AND ITS AGENTS EXPRESSLY DISCLAIM ALL SUCH REPRESENTATIONS AND WARRANTIES.** ACRAnet, its agents and its Data Providers will not be responsible or liable for any loss or damage caused by any delay or failure to provide Consumer Reports hereunder or any inaccuracy, incompleteness, or invalidity of any information in a Consumer Report, unless caused by ACRAnet's gross negligence. Client releases ACRAnet, its agents and its Data Providers harmless from all such liabilities including, without limitation, indirect, consequential, and special damages and damages for loss of profits, whether incurred by Client or any consumer or other person, whether based on contract, tort (including, without limitation, negligence, duty to warn, strict liability) warranty, or any other legal theory or on equitable grounds, even if they have been advised of the possibility of such damages. Client agrees that their maximum liability for damages in connection with a Consumer Report will not exceed an amount equal to the price paid by Client for such Consumer Report, and that the foregoing limitations, exclusions, and releases are an essential part of this Agreement and form the basis for determining the price of Consumer Reports.

VI. Client acknowledges that many services from ACRAnet's Data Providers also contain information from the Death Master File as issued by the Social Security Administration (hereinafter referred to as "DMF"); Client certifies pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F. R. § 1110.102 that consistent with Client's applicable FCRA or GLB use of ACRAnet products, use of deceased flags or other indicia within the Consumer Report 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 Client further certifies that it 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 Consumer Report.

VII. Client will pay ACRAnet, according to ACRAnet's fee schedule as in effect from time to time. ACRAnet acting through its sales agents may change fees upon written notice to Client. Client's account is delinquent if not paid in full within 30 days after the billing statement date. Upon default, Client shall pay a late charge of 1.5 percent per month on past due amounts and will be subject to suspension of Consumer Reports hereunder until all amounts owed have been paid in full at the option of ACRAnet acting through its sales agents. Client shall pay all reasonable attorneys' fees and collection costs incurred by ACRAnet or its sales agent in collecting any delinquent account, whether or not arbitration is instituted.

VIII. Either party may terminate this Agreement, without cause, with a five (5) day prior written notice to the other party. ACRAnet may terminate this Agreement immediately upon oral or written notice to Client, if Client is in breach of any of Client's obligations with respect to permissible use of, or prevention of unauthorized access to, Consumer Reports. Or if Client breaches any terms of this Agreement, including but not limited to: (a) failure to pay amounts when due, (b) violation of the Fair Credit Reporting Act; or (c) refusal to fully cooperate in allowing access of necessary records for an audit pursuant to Section II(3) of this Agreement. Any Supplements to this Agreement terminate when the Agreement terminates. The termination of this Agreement shall not terminate any of Client's obligations hereunder.

IX. Each party shall execute and deliver all such further instruments, documents and papers, and shall perform any and all acts necessary to give full

force and effect to all of the terms and provisions of this Agreement.

X. This Agreement, and all provisions hereof, shall inure to the benefit of and be binding upon the parties hereto, their respective successors in interest, assigns, administrators, executors, heirs and devisees.

XI. In the event of any dispute between or among the parties hereto respecting or arising out of this agreement, the successful or prevailing party shall be entitled to recover reasonable attorneys' fees and other costs in connection therewith, including any attorneys fees incurred after any arbitration award. An arbitration award, and any judgment entered thereon, shall include an attorneys' fees clause which shall entitle the prevailing party to recover attorneys' fees incurred to enforce the award or judgment, which attorneys' fees shall be an element of post-award or judgment costs. The parties agree that this attorneys' fees provision shall not merge into any arbitration award or judgment.

XII. No amendment or modification of this Agreement or of any covenant, condition, or limitation herein contained shall be valid unless in writing and duly executed by the party to be charged therewith.

XIII. This Agreement shall be governed by and construed in accordance with the laws of the State where the ACRAnet branch servicing this account resides and without regard to the conflicts of laws principles thereof.

XIV. Any controversy, claim or dispute between or among the parties hereto, including tort and contract claims, shall be determined by binding arbitration conducted in the county in which the ACRAnet branch servicing the account is located. The parties agree that this forum and venue is not inconvenient or improper. Arbitration shall be administered according to the state arbitration laws and procedures applicable in the county in which the arbitration occurs, and a judgment on the award may be entered in any court of competent jurisdiction. The arbitration shall be by a single arbitrator chosen by the parties, or if they cannot agree within five (5) days of exchanging names of proposed arbitrators, by a single arbitrator appointed in accordance with applicable rules and procedures. Notwithstanding any other provision of this agreement, either party may, without conflict with this arbitration provision, seek interim provisional, injunctive, or other equitable relief until the arbitration award is rendered or the controversy is otherwise resolved. The arbitrator must give effect to state statutes of limitations, such that claims will be barred from arbitration if such claims would be barred in a court proceeding under applicable statutes of limitations.

XV. Each party is duly authorized to enter into and perform this Agreement, and if such party is a corporation or limited liability company, all appropriate and necessary action has been taken by such corporation or limited liability company to authorize the signing and performance of this Agreement.

XVI. ACRAnet may assign ACRAnet's rights under this Agreement without the consent or approval of Client. Client may not assign Client's rights or delegate Client's duties under this Agreement without the prior written consent of ACRAnet. This agreement is effective when ACRAnet accepts it.

XVII Client acknowledges that it has received and reviewed a copy of the "Notice to Furnishers of Information: Obligations of Furnishers under the FCRA". (See Attachment B, Appendix N to 1022- Prescribed Notice of Furnisher Responsibilities.)

XVIII. Client acknowledges that it has received and reviewed a copy of the "Credit Scoring Services." (See Attachment C.)

XIX. Client acknowledges that it has received and reviewed a copy of the "Access Security Requirements." (See Attachment D.)

Initial here _____ Client will notify ACRAnet immediately as any approved User leaves or is terminated so that the User can be deactivated from the ACRAnet system.

XX. Client acknowledges that it has received and reviewed a copy of the "Requirements for California and Vermont Users." (See Attachment E.)

XXI. Client will address any written notice to ACRAnet required by this Agreement to President, ACRAnet, 521 West Maxwell, Spokane, WA 99201 or another address designated in writing by ACRAnet to Client. ACRAnet will address any written notice required by this Agreement to Client at the address noted below or another address designated in writing by Client to ACRAnet.

Street: _____

City: _____

State/Zip: _____

XXII. This Agreement, together with any addendum hereto, constitutes the entire Agreement between the parties, and supersedes any prior written or oral communications, proposals, and agreements with respect to such subject matter. Letter agreements may not conflict with this Agreement and may address only pricing, administrative fee, minimum monthly usage, minimum monthly charges and deposit, which shall be subject to change by ACRAnet on thirty (30) days' written notice unless otherwise specified. No changes in this Agreement or any supplement may be made except in writing by the President of ACRAnet, Inc.

Signature page to follow

Company:	_____	ACRAnet, Inc	
Signature:	_____	Signature:	_____
Name of signor:	_____ (Print or Type)	Name of signor:	_____ (Print or Type)
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Please return completed contracts to:

ACRAnet, Inc.
521 W. Maxwell
Spokane, WA 99201-2417
Attention: New Accounts Processing

Phone: 1-800-304-1249
Fax: 1-800-845-7435
Email: NewAccounts@ACRAnet.com

ATTACHMENT "A"
To: SERVICE AGREEMENT

Appendix N to Part 1022

Prescribed Notice of User Responsibilities

This appendix prescribes the content of the required notice.

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

All users of consumer reports must comply with all applicable regulations, including regulations promulgated after this notice was first prescribed in 2004. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS:
OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §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 Bureau of Consumer Financial Protection's website at www.consumerfinance.gov/learnmore. 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 Bureau's website. **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 ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. 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. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. 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. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. 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. 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. 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(f) 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.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

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)(1) 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 615(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 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 identify theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) 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 Consumer Financial Protection Bureau and the banking and credit union regulators.

The Consumer Financial Protection Bureau regulations will be available at www.consumerfinance.gov/learnmore/.

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 Consumer Financial Protection Bureau, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Consumer Financial Protection Bureau regulations may

be found at www.consumerfinance.gov/learnmore/.

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 prescribed by the Consumer Financial Protection Bureau.

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 USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If the 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).
The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

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. OBLIGATIONS WHEN 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 subjects 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 EMPLOYMEE INVESTIGATIONS

Section 603(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 agent 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 a 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. Sections 603(1), 604(c), 604(e), and 614(d). This practice is known as "prescreening" and typically involves obtaining a list of consumers from a CRA who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and 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 bearing 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 prescreened 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 appropriatenotification system.

In addition, the Consumer Financial Protection Bureau has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. <u>Disclosure and Certification Requirements</u>

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.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:

(1) the identify of all end-users;
(2) certifications from all users of each purpose for which reports will be used; and
(3) certifications 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. <u>Reinvestigations by Resellers</u>

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. <u>Fraud Alerts and Resellers</u>

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

The Consumer Financial Protection Bureau website, www.consumerfinance.gov/learnmore, 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. § 1618 et seq.:

Section 603	15 U.S.C. 1681 15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681c-1
Section 605B	15 U.S.C. 1681c-2
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 612	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 1681l
Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 1681o
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 1681r
Section 621	15 U.S.C. 1681s
Section 622	15 U.S.C. 1681s-1
Section 623	15 U.S.C. 1681s-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y

ATTACHMENT "B"
To: SERVICE AGREEMENT

Appendix M to Part 1022

Prescribed Notice of Furnisher Responsibilities

This appendix prescribes the content of the required notice.
NOTICES TO FURNISHERS OF INFORMATION:
OBLIGATIONS OF FURNISHERS UNDER THE FCRA

All furnishers of consumer reports must comply with all applicable regulations, including regulations promulgated after this notice was first prescribed in 2004. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO FURNISHERS OF INFORMATION:
OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681-1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FCRA, 15 U.S.C. § 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and may want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is set forth in full at the Bureau of Consumer Financial Protection's website at www.consumerfinance.gov/learnmore. A list of the sections of the FCRA cross-referenced to the U.S. Code is at the end of this document.

Section 623 imposes the following duties:

Accuracy Guidelines

The banking and credit union regulators and the CFPB will promulgate guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. The regulations and guidelines issued by the CFPB will be available at www.consumerfinance.gov/learnmore when they are issued. Section 623(e).

General Prohibition on Reporting Inaccurate Information

The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a)(1)(A) and (a)(1)(C).

Duty to Correct and Update Information

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must promptly provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. Section623(a)(2).

Duties After Notice of Dispute from Consumer

If a consumer notifies a furnisher, at an address specified by the furnisher for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate, the furnisher must thereafter report the correct information to CRAs. Section 623(a)(1)(B).

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. Section 623(a)(3).

The federal banking and credit union regulators and the CFPB will issue regulations that will identify when an information furnisher must investigate a dispute made directly to the furnisher by a consumer. Once these regulations are issued, furnishers must comply with them and complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." The CFPB regulations will be available at www.consumerfinance.gov. Section 623(a)(8).

Duties After Notice of Dispute from Consumer Reporting Agency

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

- Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. Sections 623(b)(1)(A) and (b)(1)(B).
- Report the results to the CRA that referred the dispute, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. Sections 623(b)(1)(C) and (b)(1)(D).
- Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).
- Promptly modify or delete the information, or block its reporting. Section 623(b)(1)(E).

Duty to Report Voluntary Closing of Credit Accounts

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. Section 623(a)(4).

Duty to Report Dates of Delinquencies

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. Section 623(a)(5).

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, by following reasonable procedures to ensure that the date reported precedes the date when the account was placed for collection, charged to profit or loss, or subjected to any similar action. Section 623(a)(5).

Duties of Financial Institutions When Reporting Negative Information

Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a)(7). The Consumer Financial Protection Bureau has prescribed model disclosures, 12 CFR Part 1022, App. B.

Duties When Furnishing Medical Information

A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agents or assignees) is a medical information furnisher for the purposes of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a)(9). This notice will enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

Duties when ID Theft Occurs

All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a)(6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each consumer reporting agency of the correct information and must thereafter report only complete and accurate information. Section 623(a)(2). When any furnisher of information is notified pursuant to the procedures set forth in Section 605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 615(f).

The Consumer Financial Protection Bureau website, www.consumerfinance.gov/learnmore, has more information about the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

	15 U.S.C.	1681	Section 615	15 U.S.C. 1681m
Section 603	15 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.	1681c-1	Section 619	15 U.S.C. 1681q
Section 605B	15 U.S.C.	1681c-2	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 614	15 U.S.C.	1681l	Section 629	15 U.S.C. 1681y

ACRANET

For ACRAnet Use Only
Company Name _____

Subscriber # _____

Attachment "C"
Credit Scoring Services

Client is a credit grantor that purchases Consumer Reports from ACRAnet pursuant to the Agreement in connection with credit transactions involving the consumer subjects of such Consumer Reports. As an enhancement to the basic Consumer Report, ACRAnet has offered Client the opportunity to purchase one or more credit risk scores provided by Trans Union, Equifax, or Experian; including, but not limited to, Fair Isaac & Co. (FICO) and Vantage score models. Use of these scoring models may require additional addendums and be subject to additional terms of use.

Client recognizes that all credit risk scores offered hereunder are statistical scores and may not be predictive as to any particular individual. No such score is intended to characterize any individual as to credit capability. Client recognizes that factors other than credit risk scores should be considered in making a credit decision, including the Credit Report, the individual credit application, economic factors, and various other pertinent information. A statement of the factors that significantly contributed to the credit risk score may accompany the score. If so, such information may be disclosed to the consumer as the reason for taking adverse action, as required by Regulation B. However, the credit risk score itself is proprietary and may not be used as the reason for adverse action under Regulation B. In addition, under the Fair Credit Reporting Act, credit risk scores are not considered part of the consumer's file. Accordingly, Client agrees only to disclose the actual credit risk score to the consumer when accompanied by the corresponding reason codes or otherwise required by law.

CLIENT HAS MADE ITS OWN ANALYSIS OF THE CREDIT RISK SCORE OR SCORES SELECTED BY CLIENT, INCLUDING THE RELIABILITY OF USING SUCH SCORES IN CONNECTION WITH CLIENTS'S CREDIT DECISION. ACRANET AND ITS AGENTS SHALL NOT BE LIABLE FOR ANY LOSS, COSTS, DAMAGES, OR EXPENSE INCURRED BY CLIENT RESULTING FROM CLIENT'S USE OF CREDIT RISK SCORES, OR THE INACCURACY THEREOF. IN NO EVENT SHALL ACRANET NOR ITS AGENTS BE LIABLE TO CLIENT FOR ANY INCIDENTAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES FOR A CLAIM BY CLIENT RESULTING FROM CLIENT'S USE OF ANY CREDIT RISK SCORE. THE TOTAL AGGREGATE LIABILITY OF ACRANET AND ITS AGENTS FOR A CLAIM BY CLIENT RELATED TO CLIENT'S USE OF ANY CREDIT RISK SCORE SHALL NOT EXCEED THE SURCHARGE PAID BY CLIENT FOR THE CREDIT RISK SCORE TO WHICH SUCH CLAIM RELATES.

Client certifies that in using the FICO/VANTAGE Credit Scoring Models that:

1. **Warranty**. Client understands that Data Providers/FICO warrants that the FICO/Vantage Scoring Model are empirically derived and demonstrably and statistically sound and that to the extent the populations to which the FICO/Vantage Scoring Models are applied is similar to the population sample on which the FICO/Vantage Scoring Models were developed, the FICO/Vantage score may be relied upon by Client to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Clients. FICO/Vantage further warrant that so long as FICO/Vantage provide the FICO/Vantage Model it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 *et seq.* THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES DATA PROVIDERS, FICO, OR VANTAGE HAVE GIVEN CLIENT WITH RESPECT TO FICO/VANTAGE SCORING MODELS AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, DATA PROVIDERS, FICO, OR VANTAGE MIGHT HAVE GIVEN CLIENT WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. Client's rights under the foregoing Warranty are expressly conditioned upon each respective Client's periodic revalidation of the FICO/Vantage Scoring Model in compliance with the requirement of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*).
2. **Release**. Client hereby releases and holds harmless ACRAnet, FICO/Vantage and/or Data Providers and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of ACRAnet, FICO/Vantage or Data Providers from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by Client resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.
3. **No License**. Nothing contained in this Agreement shall be deemed to grant Client any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by ACRAnet, Data Providers and/or FICO/Vantage or any third party involved in the delivery of the scoring services hereunder. Client acknowledges that the Data Providers/FICO/Vantage Model and its associated intellectual property rights in its output are the property of FICO/Vantage.
4. **Client Use Limitations**. By providing the Scores to Client pursuant to this Agreement, ACRAnet grants to Client a limited license to use information contained in reports generated by the Data Providers/FICO/Vantage Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing ACRAnet to deliver Scores to any third party (as may be permitted by this Agreement), Client agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the Client, and (2) identifies Data Providers and FICO/Vantage as express third party beneficiaries of such contract.
5. **Proprietary Designations**. Client shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of ACRAnet, Data Providers or FICO/Vantage or their respective affiliates, whether registered or unregistered, without such party's prior written consent.
6. **Compliance with Law**. In performing this Agreement and in using information provided hereunder, Client will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. Client certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with

applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the Client along with the Scores.

7. **Confidentiality**. Client will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. Client will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, Client will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of Client and while in transport between the parties. Client certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Data Providers's and FICO/Vantage's express written permission.
8. **Proprietary Criteria**. Under no circumstances will Client attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Data Providers and/or FICO/Vantage in performing the scoring services hereunder.
9. **Consumer Disclosure**. Notwithstanding any contrary provision of this Agreement, Client may disclose the Scores provided to Client under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.
10. **Indemnification of ACRAnet, Data Providers and FICO/Vantage**. Client will indemnify, defend, and hold each of ACRAnet, Data Providers and FICO/Vantage harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by Client of any obligations to be performed by Client under this Agreement, *provided that* Data Providers/FICO/Vantage have given Client prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.
11. **Limitation of Liability**. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL ACRANET, DATA PROVIDERS OR FICO/VANTAGE HAVE ANY OBLIGATION OR LIABILITY TO CLIENT FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY CLIENT, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT CLIENT WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ACRANET, DATA PROVIDERS OR FICO/VANTAGE TO CLIENT EXCEED THE FEES PAID BY CLIENT PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF CLIENT'S CLAIM.
12. **Third Parties**. Client acknowledges that the Scores results from the joint efforts of Data Providers and FICO/Vantage. Client further acknowledges that each Data Providers and FICO/Vantage have a proprietary interest in said Scores and agrees that either Data Providers or the FICO/Vantage may enforce those rights as required.
13. **Complete Agreement**. This Agreement sets forth the entire understanding of Client and ACRAnet with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

ACRANET

For ACRAnet Use Only
Company Name _____

Subscriber # _____

Attachment "D"
Access Security Requirements for End Users For FCRA and GLBA Data

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

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

1. Implement Strong Access Control Measures

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

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

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

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to ACRAnet's infrastructure. Each user of the system access software must also have a unique logon password.

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

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

1.7 Develop strong passwords that are:

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

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

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

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

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

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

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

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

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

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

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

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

2. Maintain a Vulnerability Management Program

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

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

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

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

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

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

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

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

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

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

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

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

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

4. 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 Safeguards Rule.

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

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

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

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

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is Company's responsibility to ensure the service provider is engaged with Experian and an exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

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

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

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

6. Regularly Monitor and Test Networks

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

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

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

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

7. Mobile and Cloud Technology

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

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

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

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

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

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

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

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

8. General

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

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to ACRAnet 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 ACRAnet 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 ACRAnet information systems; this applies to both in-house or outsourced software development) based on the following requirements:

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

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

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

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

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

8.7 Company shall report actual security violations or incidents that impact Experian to ACRAnet within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to ACRAnet of any confirmed security breach that may involve data

related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800.304.1249, Email notification will be sent to info@ACRAnet.com.

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

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

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

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

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

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

Internet Delivery Security Requirements

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

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with ACRAnet on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to ACRAnet 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 ACRAnet product based upon the legitimate business needs of each employee. ACRAnet 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 ACRAnet. 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). ACRAnet's approval of requests for (Internet) access may be granted or withheld in its sole discretion. ACRAnet 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 ACRAnet 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 ACRAnet 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 ACRAnet 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 ACRAnet's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to ACRAnet immediately.
2. As a Client to ACRAnet's 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 ACRAnet 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 ACRAnet's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding ACRAnet 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 ACRAnet 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 ACRAnet regarding access to ACRAnet's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to ACRAnet.
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 ACRAnet when needed on any system or user related matters.

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

ACRANET

For ACRAnet Use Only
Company Name _____

Subscriber # _____

Attachment "E"
Requirements for California and Vermont Users

California Users:

Provisions of the California Consumer Credit Reporting Agencies Act, as amended effective July 1, 1998, will impact the provision of consumer reports to Client under the following circumstances: (a) if Client is a "retail seller" (defined in part by California law as "a person engaged in the business of selling goods or services to retail buyers") and is selling to a "retail buyer" (defined as "a person who buys goods or obtains services from a retail seller in a retail installment sale and not principally for purpose of resale") and a consumer about whom Client is inquiring is applying, (b) in person and (c) for credit. Under the foregoing circumstances, ACRAnet, before delivering a Consumer Report to Client, must match at least three (3) items of a consumer's identification within the file maintained by the Data Providers with the information provided to Data Provider's via ACRAnet by Client in connection with the in-person credit transaction. Compliance with this law further includes Client's inspection of the photo identification of each consumer who applies for in-person credit, mailing extensions of credit to consumer responding to a mail solicitation at a specified address, taking special actions regarding a consumer's presentment of a police report regarding fraud, and acknowledging consumer demands for reinvestigations within certain time frames.

If Client is a "retail seller," Client certifies that it will instruct its employees to inspect a photo identification of the consumer at the time an application is submitted in person. If Client is not currently, but subsequently becomes a "retail seller," Client agrees to provide written notice to ACRAnet prior to ordering Consumer Reports in connection with an in-person credit transaction, and agrees to comply with the requirements of the California law as outlined in this Attachment, and with the specific certifications set forth herein.

Client certifies that, as a "retail seller," it will either (a) acquire a new Client subscriber number for use in processing Consumer Report inquiries that result from in-person credit applications covered by California law, with the understanding that all inquiries using this new Client Subscriber number will require that Client supply at least three items of identifying information form the applicant; or (b) contact Client's ACRAnet sales representative to ensure that Client's existing client number is properly coded for these transactions.

Vermont Users:

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

Vermont Certification. Client certifies that it will comply with the applicable provisions under Vermont law. In particular, Client certifies that it will order certain information relating to Vermont residents, that are Consumer Reports as defined by the VFCRA, only after Client has received prior consumer consent in accordance with the VFCRA § 2480e and applicable Vermont Rules. Client further certifies that the attached copy § 2480e of the Vermont Fair Credit Reporting Statute was received from ACRAnet.

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 the 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**

(a) 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.

(b) 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 credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent.