



The Information Network

www.ACRAnet.com

For ACRAnet Use Only	
Company Name	_____
Subscriber #	117-_____

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:

- A. Client will only use the permissible purpose as outlined within the ACRAnet Client Service Agreement (hereinafter referred to as “Agreement”) and the Application for Service in accordance with the FCRA to obtain the information derived from the Fair Isaac and Company Scoring Model (hereinafter referred to as “FICO”) or the Vantage Scoring Model.
- B. Client will limit Client’s use of the scores and reason codes solely to use in Clients own business with no right to transfer or otherwise sell, license, sublicense or distribute said scores or reason codes to third parties.
- C. Client will maintain internal procedures to minimize the risk of unauthorized disclosure and agree that such scores and reason codes will be held in strict confidence and disclosed only to those employees with a “need to know” and to no other person.
- D. Notwithstanding any contrary provision of the Agreement, Client may disclose the scores provided to Client under the Agreement to the consumer, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only as required by law.
- E. Client will comply with all applicable laws and regulations in using the scores and reason codes purchased from ACRAnet.
- F. Client or any of its employees, agents or subcontractors will not use any trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of the Data Providers or Fair, Isaac and Company, or their affiliates without such entity’s prior written consent.
- G. Client will not in any manner, directly or indirectly attempt to discover or reverse engineer any confidential and proprietary criteria developed or used by the Data Providers/Fair, Isaac in performing the FICO/Vantage Scoring Model.
- H. 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 MERCHANTABILITY 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.*).
- I. Client agrees that the aggregate liability of the Data Providers/FICO to the Client is equal to the lesser of the Fees paid by ACRAnet to the Data Providers/FICO for the FICO/Vantage Scoring Models resold to the pertinent Client during the six (6) month period immediately preceding the Client’s claim, or the fees paid by the pertinent Client to ACRAnet under the Agreement during said six (6) month period and excluding any liability of the Data Providers/FICO for incidental, indirect, special or consequential damages of any kind.



For ACRAnet Use Only

Company Name _____

Subscriber # _____

Access Security Requirements

User Security

Due to heightened security conditions associated with Internet access and connectivity, Client must agree to the following stipulations. **1)** Client understands that the provider #, User ID #, Client # and password provided by ACRAnet secure their Internet based access; and that the security of this access is guarded by their Windows login password. Client agrees to keep this access secure by keeping their login information private. **2)** Client agrees that after using ACRAnet's Internet access Client will logoff. Client agrees to abide by the terms and conditions stated herein.

It is a requirement that all end users (Clients) take precautions to secure any system or device used to access consumer credit information. To that end, the following requirements have been established.

A. Implement Strong Access Control Measures

- (1) Client will not provide any Subscriber Codes or any of the above ID information or passwords to anyone. The Data Providers will never contact the Client and request the Subscriber Code number or password.
- (2) Proprietary or third party system access software must have Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known to only supervisory personnel.
- (3) Client must request that Subscriber Code password be changed immediately when:
 - i. Any system access software is replaced by another system access software or is no longer used;
 - ii. The hardware on which the software resides is upgraded, changed or disposed of
- (4) Protect Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- (5) Create a separate, 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.
- (6) Ensure that user ID's are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- (7) Keep user passwords confidential.
- (8) Develop strong passwords that are:
 - i. Not easily guessable (e.g. your name or company name, repeating numbers and letters or consecutive numbers and letters);
 - ii. Contain a minimum of eight (8) alpha/numeric characters for standard user accounts
- (9) Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- (10) Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- (11) Restrict the number of key personnel who have access to credit information.
- (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 ACRAnet Application for Service and the Client Service Agreement.
- (13) Ensure that Client and Client's employees do not access their own consumer 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.
- (14) Implement a process to terminate access right immediately for users who access ACRAnet information when those users are terminated or when they have a change in their job tasks and no longer require access consumer information.
- (15) After normal business hours, turn off and lock all devices or systems used to obtain consumer information.
- (16) Implement physical security controls to prevent unauthorized entry to Client's facility and access to systems used to obtain consumer report information.

B. Maintain a Vulnerability Management Program

- (1) Keep operating system(s), firewalls, routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- (2) Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, ID's and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- (3) Implement and follow current best security practices for computer virus detection scanning services and procedures:
 - i. Use, implement and maintain a current, commercially available computer virus detection/scanning product on all computers, systems and networks.
 - ii. If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
 - iii. On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- (4) Implement and follow current best security practices for computer anti-spyware scanning services and procedures:
 - i. Use, implement and maintain a current, commercially available computer anti-spyware scanning product on all computers, systems and networks.
 - ii. If you suspect actual or potential spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.

- iii. Run a secondary anti-spyware scan upon completion of the first scan to ensure all spyware has been removed from your computers.
- iv. Keep anti-spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the internet (which prevents access to some known problematic sites), then it is recommended that anti-spyware scans be completed more frequently than weekly.

C. Protect Data

- (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 (e.g. tape, disk, paper, etc.).
- (2) All information provided by the Data Providers is classified as confidential and must be secured to this requirement at a minimum.
- (3) Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- (4) Encrypt all ACRAnet data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- (5) Only open e-mail attachments and links from trusted sources and after verifying legitimacy.

D. Maintain an Information Security Policy

- (1) Develop and follow a security plan to protect the confidentiality and integrity of the personal consumer information as required under the GLB Safeguard Rule.
- (2) Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- (3) The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- (4) Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

E. Build and Maintain a Secure Network

- (1) Protect Internet connection with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.
- (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.
- (3) Administrative access to firewalls and servers must be performed through a secure internal wired connection only.
- (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) Encrypt Wireless access points with a minimum of WEP 128 bit encryption and/or WPA encryption where available.
- (6) Disable vendor default passwords, service set identifier and IP Addresses on wireless access points and restrict authentication on the configuration of the access point.

F. Regularly Monitor and Test Networks

- (1) Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- (2) Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide services hereunder to access ACRAnet systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access to penetration or exposure to an unauthorized third party by:
 - i. Protecting against intrusions;
 - ii. Securing the computer systems and network devices;
 - iii. And protecting against intrusions of operating systems or software.

G. Unauthorized Access

- (1) In the event of an unauthorized access there will be a thorough investigation as to the root cause; Client agrees to help facilitate the investigation fully.
- (2) Once the cause of the unauthorized access is determined, Client may be required to assume responsibility for costs associated with the unauthorized access and additional conditions may be established in order for ACRAnet to continue to provide Consumer Reports to Client.

For ACRAnet Use Only
Company Name _____
Subscriber # _____

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 from 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 hereby 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.

Company: _____

ACRAnet, Inc

Signature: _____

Signature: _____

Name of signor: _____
(Print or Type)

Name of signor: _____
(Print or Type)

Title: _____

Title: _____

Date: _____

Date: _____