

FCRA REQUIREMENTS

Federal Fair Credit Reporting Act (as amended by the Consumer Credit Reporting Reform Act of 1996) Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. We suggest you and your employees become familiar with the following sections in particular:

- 604. Permissible Purpose of Reports
- 607. Compliance Procedures
- 615. Requirements on users of consumer's reports
- 616. Civil liability for willful noncompliance
- 617. Civil liability for negligent noncompliance
- 618. Obtaining information under false pretenses
- 621. Administrative Enforcement
- 622. Responsibilities of Furnishers of Information to Consumer Reporting Agencies

Each of these sections is of direct consequences to users who obtain reports on consumers. As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as an investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

Trans Union, Equifax and Experian strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce. In addition to the Federal Fair Credit Reporting Act other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate. We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

AUTHORIZED SIGNATURE

DATE

TransUnion/Fair Isaac Score Addendum

CLASSICSM CREDIT RISK SCORE SERVICES

1. Based on an agreement with Trans Union LLC ("Trans Union") and Fair Isaac Corporation ("Fair Isaac"), Service 1st has access to a unique and proprietary statistical credit scoring service jointly offered by Trans Union and Fair Isaac which evaluates certain information in the credit reports of individual consumers from Trans Union's data base ("Classic") and provides a score which rank orders consumers with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring (the "Classic Score").
2. Client, from time to time, may desire to obtain Classic Scores from Trans Union via an on-line mode in connection with consumer credit reports.
3. Client has previously represented and now, again represents that it is a _____ and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").
4. Client certifies that it will request Classic Scores pursuant to procedures prescribed by Service 1st from time to time only for the permissible purpose certified above, and will use the Classic Scores obtained for no other purpose.
5. Client will maintain copies of all written authorizations for a minimum of three (5) years from the date of inquiry.
6. Client agrees that it shall use each Classic Score only for a one-time use and only in accordance with its permissible purpose under the FCRA.
7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, Service 1st may, upon its election, discontinue serving the Client and cancel this Agreement, in whole or in part (e.g., the services provided under this Addendum only) immediately.
8. Client recognizes that factors other than the Classic Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors.
9. Trans Union and Fair Isaac shall be deemed third party beneficiaries under this Addendum.
10. Up to five score reason codes, or if applicable, exclusion reasons, are provided to Client with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg. B"). However, the Classic Score itself is proprietary to Fair Isaac, may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party, except: (1) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (2) as clearly required by law. Client will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and Trans Union's prior written consent
11. In the event Client intends to provide Classic Scores to any agent, Client may do so provided, however, that Client first enters into a written agreement with such agent that is consistent with Client's obligations under this Agreement. Moreover, such agreement between Client and such agent shall contain the following obligations and

- acknowledgments of the agent: (1) Such agent shall utilize the Classic Scores for the sole benefit of Client and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit; (2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party without Trans Union and Fair Isaac's prior written consent except (a) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (b) as clearly required by law; (3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration; (4) Such agent shall not resell the Classic Scores; and (5) Such agent shall not use the Classic Scores to create or maintain a database for itself or otherwise.
12. Client acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information, will result in an inquiry being added to the consumer's credit file.
 13. Client shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject.
 14. The information including, without limitation, the consumer credit data, used in providing Classic Scores under this Agreement were obtained from sources considered to be reliable. However, due to the possibilities of errors inherent in the procurement and compilation of data involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed. Moreover, in no event shall Trans Union, Fair Isaac, nor their officers, employees, affiliated companies or bureaus, independent contractors or agents be liable to Client for any claim, injury or damage suffered directly or indirectly by Client as a result of the inaccuracy or incompleteness of such information used in providing Classic Scores under this Agreement and/or as a result of Client's use of Classic Scores and/or any other information or serviced provided under this Agreement.
 - 15.1 Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to Trans Union and used in the computation of the Classic Score ("Models") are empirically derived from Trans Union's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and Regulation B promulgated thereunder. Classic provides a statistical evaluation of certain information in Trans Union's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring relative to other individuals in Trans Union's database. The score may appear on a credit report for convenience only, but is not a part of the credit report nor does it add to the information in the report on which it is based.
 - 15.2 THE WARRANTIES SET FORTH IN SECTION 15.1 ARE THE SOLE WARRANTIES MADE UNDER THIS ADDENDUM CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANS UNION MAKE ANY OTHER REPRESENTATIONS OR WARRANTIES CONCERNING THE PRODUCTS AND SERVICES TO BE PROVIDED UNDER THIS AGREEMENT OTHER THAN AS SET FORTH IN THIS ADDENDUM. THE WARRANTIES AND REMEDIES SET FORTH IN SECTION 15.1 ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR

DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

16. IN NO EVENT SHALL ANY PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY THE OTHER PARTIES AND ARISING OUT OF THE PERFORMANCE OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF GOOD WILL AND LOST PROFITS OR REVENUE, WHETHER OR NOT SUCH LOSS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.
17. THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO CLIENT, IN NO EVENT SHALL THE AFORESTATED LIMITATIONS OF LIABILITY, SET FORTH ABOVE IN SECTION 16, APPLY TO DAMAGES INCURRED BY TRANS UNION AND/OR FAIR ISAAC AS A RESULT OF: (A) GOVERNMENTAL, REGULATORY OR JUDICIAL ACTION(S) PERTAINING TO VIOLATIONS OF THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM CLIENT'S BREACH, DIRECTLY OR THROUGH CLIENT'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT.
18. ADDITIONALLY, NEITHER TRANS UNION NOR FAIR ISAAC SHALL BE LIABLE FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL TRANS UNION'S AND FAIR ISAAC'S AGGREGATE TOTAL LIABILITY, IF ANY, UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY CLIENT DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS (\$10,000.00), WHICHEVER AMOUNT IS LESS.
19. This Addendum may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this Addendum by Client; (2) in the event the agreement(s) related to Classic between Trans Union, Fair Isaac and Service 1st are terminated or expire; (3) in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation by any governmental entity.

Date: _____

Date: _____

Service 1st Information Systems, Inc.(AGENCY)

"Client"

Signature

Title

Vermont Fair Credit Reporting Statue, 9 V.S.A. 2480c (1999)

2480 c. 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 subscription (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 government 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.

_____ Initials

BUSINESSES THAT CANNOT BE PROVIDED INFORMATION

Adult entertainment services of any kind

Business that operates out of an apartment or unrestricted location within a residence (unless approved by repository)

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

Bail Bondsman

Check cashing establishment

Credit counseling

Credit repair clinic

Dating Service

Financial Counseling

Genealogical or heir research firm

Massage Services

Company that locates missing children

Pawn shop

Private Detectives, detectives agencies or investigative companies

Individual seeking information for their private use

Company that handles third-party repossession

Company or individual involved in spiritual counseling

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

Tattoo service

Insurance claims

Internet locator services

Asset location services

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

New agencies or journalists

Law enforcement (except for employment screening purposes)

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

Companies listed on repository alert report notifications

_____ Initials

LETTER OF INTENT

A letter of Intent must be submitted on your company letterhead and must be signed by an officer, owner or authorized manager of your company. The Letter of Intent must include, at a minimum, the following information:

- **The nature of your business**
- **Your intended use for the services**
- **Your anticipated monthly volume**
- **Intent as to whether it anticipates its access to be primarily local, regional, or national**

**LIST OF LENDERS YOU REISSUE TO ON COMPANY
LETTERHEAD**

On your company letterhead, list the names and contact numbers of lenders you will be reissuing credit reports to. If you will not be reissuing credit reports, please write on company letterhead that you will not be reissuing credit reports.

IP Addresses:

Please list ALL IP addresses from your computers that will have Service 1st downloaded(you can get this by going to www.mclsupport.com)

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11. _____

12. _____

13. _____

14. _____

15. _____

16. _____

17. _____

18. _____

EXPERIAN CREDIT SCORING SERVICES ADDENDUM

This Credit Scoring Services Agreement, (“Agreement”), dated: _____,
between
_____ (“End User”) and Service 1st Information Systems
 (“Provider”)

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc. (“Experian”); and

WHEREAS, Experian and Fair Isaac Corporation (“Fair, Isaac”) offer the “Experian/Fair, Isaac Model”, consisting of the application of a risk model developed by Experian and Fair, Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering into a credit relationship will result in a numerical score (the “Score” and collectively, “Scores”); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, for good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

1. General Provisions

A. Subject of Agreement. The subject of this Agreement is End User’s purchase of Scores produced from the Experian/Fair, Isaac Model from Provider.

B. Application. This Agreement applies to all uses of the Experian/Fair, Isaac Model by End User during the term of this agreement.

C. Term. The term of this Agreement (the “Term”) is the period consisting of the Initial Term and, if this Agreement is renewed, the Renewal Term(s), as follows:

(1) Initial Term. The “Initial Term” is the period beginning at 12:01 a.m. on the date written above and shall continue on a month to month basis.

(2) Renewal Term(s). Unless one or both of the parties delivers written notice of such party’s (parties”) intent not to renew no later than thirty (30) days before the end of the Initial Term, this agreement shall be automatically renewed on a month to month basis.

2. Experian/Fair, Isaac Score

A. Generally. Upon request by End User during the Term, Provider will provide End User with the Scores.

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

WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CRF Section 202 et seq.).

C. Release. End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Experian from liability for any damages, losses, costs or expenses whether direct or indirect, suffered or incurred by End User 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. Fees. See product pricing page.

4. Intellectual Property

A. No License. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.

B. End User Use Limitations. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair, Isaac as express third party beneficiaries of such contract.

C. Proprietary Designations. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of Provider, Experian or Fair, Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

5. Compliance and Confidentiality

A. Compliance with Law. In performing this Agreement and in using information provided hereunder, End User 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. End User 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 End User along with the Scores.

B. Confidentiality. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder, End User 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, End User 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 End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian’s and Fair, Isaac’s express written permission.

C. Proprietary Criteria. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

D. Consumer Disclosure. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User 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.

6. Indemnification and Limitations

A. Indemnification of Provider, Experian and Fair, Isaac. End User will indemnify, defend, and hold each of Provider, Experian and Fair, Isaac 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 End User of any obligations to be performed by End User under this Agreement, provided that Experian/Fair, Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

B. Limitation of Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

7. Miscellaneous

A. Third Parties. End User acknowledges that the Scores results from the joint efforts of Experian and Fair, Isaac. End User further acknowledges that each Experian and Fair, Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair, Isaac may enforce those rights as required.

B. Complete Agreement. This Agreement sets forth the entire understanding of End User and Provider with respect to the subject matter hereof and supersedes all prior letter of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

Signature

Date

Print Name/Title

Company

-

ACCESS SECURITY REQUIREMENTS

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

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

1. Implement Strong Access Control Measures

- i. Do not provide your credit reporting agency Subscriber Code(s) or password(s) to anyone. No one from the credit-reporting agency will ever contact you and request your Subscriber Code number or password.
- ii. Proprietary or third party system access software must have credit reporting agency Subscriber Code(s) and password(s) hidden or embedded. Account numbers and password(s) should be known only by supervisory personnel.
- iii. You must request your Subscriber Code password 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 of.
- iv. Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- v. Create a separate, unique Login for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon on password.
- vi. Ensure that User IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- vii. Keep User password(s) confidential.
- viii. 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 seven (7) alpha/numeric characters for standard user accounts
- ix. Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
 - x. Active logins to credit information systems must be configured with a thirty (30) minute inactive session, timeout.
 - xi. Restrict the number of key personnel who have access to credit information.
 - xii. Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
 - xiii. Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
 - xiv. Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
 - xv. After normal business hours, turn off and lock all devices or systems used to obtain credit information.
 - xvi. Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

- i. Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- ii. Configure infrastructure(s) such as Firewalls, Routers, personal computers, and similar] components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

- iii. Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
 - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
 - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
 - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- iv. Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
 - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
 - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computer.
 - 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 sties), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

3. Protect Data

- i. 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.)
- ii. All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum.
- iii. Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

- iv. Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- v. Only open email attachments and links from trusted sources and after verifying legitimacy.

4. Maintain an Information Security Policy

- i. Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the *GLB Safeguard Rule*.
- ii. 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.
- iii. 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.
- iv. Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

5. Build and Maintain a Secure Network

- i. Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- ii. 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.
- iii. Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- iv. 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.
- v. Encrypt Wireless access points with a minimum of WEP 128-bit encryption, WPA encryption where available.
- vi. Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

6. Regularly Monitor and Test Networks

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

Record Retention: *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application and if applicable, a purchase agreement for a period of not less than 60 months. When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.*

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

I agree to implement and adhere to the above controls.

Date

Signature

Company Name

Print Name/Title

Account number / Subscriber code: _____

Glossary

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 it's 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.

SSID - Part of the Wi-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part of that network. Wireless devices that communicate with each other share the same SSID.

Subscriber Code - Your credit reporting agency account number.

WEP Encryption - (Wired Equivalent Privacy) a part of the wireless networking standard intended to provide secure communication. The longer the key used, the stronger the encryption will be. Older technology reaching its end of life.

WPA - (Wi-Fi Protected Access) A part of the wireless networking standard that provides stronger authentication and more secure communications. Replaces WEP. Uses dynamic key encryption verses static as in WEP (key is constantly changing and thus more difficult to break than WEP).

(January 2009)

ON-SITE INSPECTION AUTHORIZATION

Due to compliance requirements from Trans Union, Experian and Equifax, a complete on-site inspection of all client offices must be conducted by a repository approved third-party on-site inspection company. These companies have been given complete training, guidance and instructions by each repository on their specific inspection guidelines. The purpose of this on-site inspection is to ensure that the business: 1) is a bona fide business entity operating in an appropriate business location for the purpose listed on their Service 1st application, 2) adheres to access security requirements and appropriate security of confidential consumer credit information, and 3) possesses and displays appropriate signage and state and industry licenses.

I authorize Service 1st Information Systems to order and conduct a third party inspection of the provided office location. The address provided is (please check one) an Office ____ / a Residence _____. I understand that the cost for this visit is \$75.00 and hereby authorize Service 1st Information Systems to collect this amount by charging the credit card listed below. This authorization is for the purpose of the on-site inspection charge **only** and does not constitute an authorization for charges for any other purpose:

Company Name: _____

Company Address: _____

City, State, Zip: _____

I do hereby certify that I am an authorized signer on the aforementioned credit card and do fully consent to the terms of the herein authorization.

Signature: _____ Date: _____

Note: To ensure a timely scheduling of the on-site inspection, please provide the name(s) and contact information of the individuals within your office who may be contacted during normal business hours.

Contact Name: _____ Phone: _____

Cell: _____ Email: _____

Alt. Contact Name: _____ Phone: _____

Cell: _____ Email: _____

(Complete only if different from credit card information provided on previous page)

CREDIT CARD TO BE USED FOR PAYMENT OF ON-SITE INSPECTION ONLY

I do hereby authorize Service 1st Information Systems to debit the following credit card

Credit Card Type: Visa MC Amex Discover

Credit Card #: _____ Exp: ____/____

Name on Card: _____

Mailing Address on card: _____

City, State, Zip: _____

I do hereby certify that I am an owner of authorized user of the aforementioned credit card and do fully consent to the terms of the herein authorization.

Signature of Cardholder: _____ Date: _____