control of the Customer (i.e., employee fraud, misconduct or abuse; access by an unqualified or improperly qualified user; improperly secured website, etc.), Customer may be assessed an expense recovery fee.

Experian Access Security Requirements

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, 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. Experian reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

1. Implement Strong Access Control Measures

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

1.2 If using third party or proprietary system to access Experian'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 Experian data/systems.

1.3 If the third party or third party software, proprietary system or software, used to access Experian data/systems, is replaced or no longer is 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 Experian'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:

- o are not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive number and letters);
- o contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts; and
- o for interactive sessions, (i.e. non system-to-system), ensure that password(s) are changed periodically (every 90 days is recommended).

1.8 Passwords, (e.g. subscriber code passwords, user password), must be changed immediately when: n any system access software is replaced by another system access software or is no longer used;

- o the hardware on which the software resides is upgraded, changed or disposed; and/or
- o 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 file/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow the 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; and/or
  - 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 Credit Technologies, Inc. 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 Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and 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. Any stand-

5.4 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 Experian 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 Experian 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; and
- 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; and
- 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 Experian 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 Experian 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 Experian 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 Experian 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:

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 Experian 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 Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian 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 Experian product based upon the legitimate business needs of each employee. Experian 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 Experian. 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/pass-phrases (this also applies to the unique Server-to- Server access IDs and passwords/pass-phrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian 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/pass-phrases 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 Credit Technologies, Inc. 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 Experian 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 Experian on information and product access, in accordance with these Experian Access Security Requirements. 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 Experian's systems and information (via the Internet). Changes in Head Security Designate status, (e.g. transfer or termination), are to be reported to Credit Technologies, Inc. immediately.

2. As a Client to Experian'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 Experian 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 Experian's Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding Experian 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 Experian products and services.

5. Must disable Authorized User ID if it becomes compromised or if company terminates the Authorized User's employment.

6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.

7. Shall immediately report changes in their Head Security Designate's status, (e.g. transfer ortermination.)

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 Experian when needed on any system or user related matters.

Certify that the client shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to:

(i) insure the security and confidentiality of the information provided by Reseller,
(ii) protect against any anticipated threats or hazards to the security or integrity of such information, and
(iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

Reseller must use the complete entire wording stated above or language substantially similar within the contract with the end user.

Certify that the client is the end user and will not further sell the information.

Acknowledge that many services containing Experian information also contain information from the Death Master File as issued by the Social Security Administration ("DMF"); certify pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102 that, consistent with its applicable FCRA or GLB use of Experian information, the client's use of deceased flags or other indicia within the Experian information is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1); and certify that the client will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian information.

Exhibit D

TRANS UNION REQUIREMENTS

Customer, in order to receive consumer credit information from Trans Union, LLC, through CTI, agrees to comply with the following conditions required by Trans Union, which may be in addition to those outlined in the Customer Service Agreement ("Agreement"). Customer understands and agrees that Trans Union's delivery of information to Customer via CTI is specifically conditioned upon Customer's agreement with the provisions set forth in this Agreement. Customer understands and agrees that these requirements pertain to all of its employees, managers and owners and that all persons having access to Trans Union consumer credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

1. Customer certifies that Customer shall use the consumer reports:

   (a) solely for the Subscriber's certified use(s); and

   (b) solely for Customer's exclusive one-time use.

   Customer shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with Customer's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by Customer only to Customer's designated and authorized employees having a need to know and only to the extent necessary to enable Customer to use the Consumer Reports in accordance with this agreement. Customer shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.

2. Customer will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

3. Customer shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that Customer may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its Customer for scores obtained from Trans Union, or as explicitly otherwise authorized in advance and in writing by Trans Union through Reseller, Customer shall not disclose to consumers or any third party, any or all such scores provided under such agreement, unless clearly required by law.

4. With just cause, such as violation of the terms of the Customer's contract or a legal requirement, or a material change in existing legal requirements that adversely affects the Customer's agreement, Reseller may, upon it selection, discontinue serving the Customer and cancel the agreement immediately.

5. Customer will request Scores only for Customer's exclusive use. Customer may store Scores solely for Customer's own use in furtherance of Customer's original purpose for obtaining the Scores. Customer shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except:

   (i) to those employees of Customer with a need to know and in the course of their employment;

   (ii) to those third party processing agents of Customer who have executed an agreement that limits the use of the Scores by the third party to the use permitted to Customer and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering;

   (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or

   (iv) as required by law.

6. Customer hereby agrees to comply with all current and future policies and procedures instituted by CTI and required by Trans Union. CTI will give Customer as much notice as possible prior to the effective date of any such new policies required in the future, but does not guarantee that reasonable notice will be possible. Customer may terminate this agreement at any time after notification of a change in policy in the event Customer deems such compliance as not within its best interest.

7. Customer certifies that it is not a reseller of the information, a private detective, bail bondsman, attorney, credit counseling firm, financial counseling firm, credit repair clinic, pawn shop (except companies that do only Title pawn), check cashing company, genealogical or heir research firm, dating service, massage or tattoo service, business that operates out of an apartment, an individual

seeking information for his private use, an adult entertainment service of any kind, a company that locates missing children, a company that handles third party repossession, a company seeking information in connection with time shares or subscriptions, a company or individual involved in spiritual counseling or a person or entity that is not an end-user or decision-maker, unless approved in writing by Trans Union.

8. Customer agrees that Trans Union shall have the right to audit records of Customer that are relevant to the provision of services set forth in this agreement. Customer authorizes CRA to provide to Trans Union, upon Trans Union's request, all materials and information relating to its investigations of Customer and agrees that it will respond within the requested time frame indicated for information requested by Trans Union regarding Trans Union information. Customer understands that Trans Union may require CRA to suspend or terminate access to Trans Union's information in the event Customer does not cooperate with any such an investigation. Customer shall remain responsible for the payment for any services provided to Customer prior to any such discontinuance.

9. Customer agrees that Trans Union information will not be forwarded or shared with any third party unless required by law or approved by Trans Union. If approved by Trans Union and authorized by the consumer, Customer may deliver the consumer credit information to a third party, secondary, or joint user with which Customer has an ongoing business relationship for the permissible use of such information. Customer understands that Trans Union may charge a fee for the subsequent delivery to secondary users.

10. Trans Union shall use reasonable commercial efforts to obtain, assemble and maintain credit information on individuals as furnished by its subscribers or obtained from other available sources.

11. THE WARRANTY SET FORTH INTHE PREVIOUS SENTENCE IS THE SOLE WARRANTY MADE BY TRANS UNION CONCERNING THE CONSUMER REPORTS, INCLUDING, BUT NOT LIMITED TO THE TU SCORES. TRANS UNION MAKES NOOTHER REPRESENTATIONS OR WARRANTIES INCLUDING, BUT NOT LIMITED TO, ANY REPRESENTATIONS OR WARRANTIES REGARDING THE ACCURACY, COMPLETENESS, OR BOTH, OF ANY AND ALL OF THE AFOREMENTIONED PRODUCTS AND SERVICES THAT MAY BE PROVIDED TO CRA. THE WARRANTY SET FORTH IN THE FIRST SENTENCE OF THIS PARAGRAPH IS IN LIEU OF ALL OTHER WARRANTIES, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, BUT NOT LIMITED TO, 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.

Exhibit E

LEXISNEXIS® RISK SOLUTIONS REQUIREMENTS

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

1. The nature of User's business is mortgage lending.
2. User orders Consumer Reports Credit Technologies for the following purpose(s) under the Fair Credit Reporting Act and such reports will not be used for any other purpose:

   For the extension and/or review of credit to the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681(b)(a)(3)(A).

1. RESTRICTED LICENSE. Credit Technologies Inc. hereby grants to Customer a restricted license to use the Credit Technologies Inc. Services and any data contained therein, subject to the restrictions and limitations set forth below:

(i) **Generally.** Credit Technologies Inc. hereby grants to Customer a restricted license to use the Credit Technologies Inc. Services solely for Customer's own internal business purposes. Customer represents and warrants that all of Customer's use of the Credit Technologies Inc. Services shall be for only legitimate business purposes, including those specified by Customer in connection with a specific information request, relating to its business and as otherwise governed by the Agreement. Customer shall not use the Credit Technologies Inc. Services for marketing purposes, resell, or broker the Credit Technologies Inc. Services to any third party and shall not use the Credit Technologies Inc. Services for personal (non-business) purposes. Customer shall not use the Credit Technologies Inc. Services to provide data processing services to third-parties or evaluate the data of or for third-parties. Customer agrees that if Credit Technologies Inc. determines or reasonably suspects that continued provision of Credit Technologies Inc. Services to Customer entails a potential security risk, or that Customer is engaging in marketing activities, reselling, brokering or processing or evaluating the data of or for third-parties, or using the Credit Technologies Inc. Services for personal (non-business) purposes or using the Credit Technologies Inc. Services' information, programs, computer applications, or data, or is otherwise violating any provision of this Agreement, or any of the laws, regulations, or rules described herein, Credit Technologies Inc. may take immediate action, including, without limitation, terminating the delivery of, and the license to use, the Credit Technologies Inc. Services. Customer shall not access the Credit Technologies Inc. Services from Internet Protocol addresses located outside of the United States and its territories without Credit Technologies Inc.'s prior written approval. Customer may not use the Credit Technologies Inc. Services to create a competing product. Customer shall comply with all laws, regulations and rules, which govern the use of the Credit Technologies Inc. Services and information provided therein. Credit Technologies Inc. may at any time mask or cease to provide Customer access to any Credit Technologies Inc. Services or portions thereof, which Credit Technologies Inc. may deem, in Credit Technologies Inc.'s sole discretion, to be sensitive or restricted information.

(ii) **GLBA Data.** Some of the information contained in the Credit Technologies Inc. Services is "nonpublic personal information," as defined in the Gramm-Leach-Bliley Act (15 U.S.C. § 6801, et seq.) and related state laws, (collectively, the "GLBA"), and is regulated by the GLBA ("GLBA Data"). Customer shall not obtain and/or use GLBA Data through the Credit Technologies Inc. Services, in any manner that would violate the GLBA, or any similar state or local laws, regulations and rules. Customer acknowledges and agrees that it may be required to certify its permissible use of GLBA Data falling within an exception set forth in the GLBA at the time it requests information in connection with certain Credit Technologies Inc. Services and will recertify upon request by Credit Technologies Inc. Customer certifies with respect to GLBA Data received through the Credit Technologies Inc. Services that it complies with the Interagency Standards for Safeguarding Customer Information issued pursuant to the GLBA.

(iii) **DPPA Data.** Some of the information contained in the Credit Technologies Inc. Services is "personal information," as defined in the Drivers Privacy Protection Act (18 U.S.C. § 2721, et seq.) and related state laws, (collectively, the "DPPA"), and is regulated by the DPPA ("DPPA Data"). Customer shall not obtain and/or use DPPA Data through the Credit Technologies Inc. Services in any manner that would violate the DPPA. Customer acknowledges and agrees that it may be required to certify its permissible use of DPPA Data at the time it requests information in connection with certain Credit Technologies Inc. Services and will recertify upon request by Credit Technologies Inc.

(iv) **Social Security and Driver's License Numbers**. Credit Technologies Inc. may in its sole discretion permit Customer to access QA Data (as previously defined). If Customer is authorized by Credit Technologies Inc. to receive QA Data, and Customer obtains QA Data through the Credit Technologies Inc. Services, Customer certifies it will not use the QA Data for any purpose other than as expressly authorized by Credit Technologies Inc. policies, the terms and conditions herein, and applicable laws and regulations. In addition to the restrictions on distribution otherwise set forth in

Paragraph 2 below, Customer agrees that it will not permit QA Data obtained through the Credit Technologies Inc. Services to be used by an employee or contractor that is not an Authorized User with an Authorized Use. Customer agrees it will certify, in writing, its uses for QA Data and recertify upon request by Credit Technologies Inc. Customer may not, to the extent permitted by the terms of this Agreement, transfer QA Data via email or ftp without Credit Technologies Inc.'s prior written consent. However, Customer shall be permitted to transfer such information so long as:

1) a secured method (for example, sftp) is used,
2) transfer is not to any third-party, and
3) such transfer is limited to such use as permitted under this Agreement.

Credit Technologies Inc. may at any time and for any or no reason cease to provide or limit the provision of QA Data to Customer.

(v) **Copyrighted and Trademarked Materials.** Customer shall not remove or obscure any trademarks, copyright notices or other notices contained on materials accessed through the Credit Technologies Inc. Services.

(vi) **National Change of Address Database.** Credit Technologies Inc. is a licensee of the United States Postal Service's NCOALINK database ("NCOA Database"). The information contained in the NCOA Database is regulated by the Privacy Act of 1974 and may be used only to provide a mailing list correction service for lists that will be used for preparation of mailings. If Customer receives all or a portion of the NCOA Database through the Credit Technologies Inc. Services, Customer hereby certifies to Credit Technologies Inc. that it will not use such information for any other purpose. Prior to obtaining or using information from the NCOA Database, Customer agrees to complete, execute and submit to Credit Technologies Inc. the NCOA Processing Acknowledgement Form.

(vii) **Additional Terms.** Certain materials contained within the Credit Technologies Inc. Services are subject to additional obligations and restrictions. Without limitation, these services include news, business information (e.g., Dun & Bradstreet reports), and federal legislative and regulatory materials. To the extent that Customer receives such materials through the Credit Technologies Inc. Services, Customer agrees to comply with the General Terms and Conditions for Use of Credit Technologies Inc. Services contained at the following website: www.lexisnexis.com/terms/general (the "General Terms"). The General Terms are hereby incorporated into this Agreement by reference.

(viii) **Fair Credit Reporting Act Obligations.** Customer certifies that when using the Credit Technologies Inc. Services, it will comply with all applicable provisions of the FCRA and all other applicable federal, state and local legislation, regulations and rules. Without limiting the generality of the foregoing, Customer certifies that:

(a) Customer will comply with all applicable provisions of the California Credit Reporting Agencies Act and any related regulations; and

(b) Customer will comply with all Vermont statutes and regulations on fair credit reporting, including but not limited to, obtaining the consent of Vermont residents prior to obtaining any information on Vermont residents through these Credit Technologies Inc. Services. In addition, Customer certifies it has a permissible purpose under the FCRA for obtaining a Consumer Report as set forth in this Agreement. Customer acknowledges that Credit Technologies Inc. has provided the "Notice to Users of Consumer Reports", attached hereto as Attachment A, which informs users of consumer reports of their legal obligations under the FCRA.

(ix) **MVR Data.** If Customer is permitted to access Motor Vehicle Records ("MVR Data") from Credit Technologies Inc., without in any way limiting Customer's obligations to comply with all state and federal laws governing use of MVR Data, the following specific restrictions apply and are subject to change:

(a) Customer shall not use any MVR Data provided by Credit Technologies Inc., or portions of information contained therein, to create or update a file that Customer uses to develop its own source of driving history information.

(b) As requested by Credit Technologies Inc., Customer shall complete any state forms that Credit Technologies Inc. is legally or contractually bound to obtain from Customer before providing Customer with MVR Data.

(c) Credit Technologies Inc. (and certain Third-Party vendors) may conduct reasonable and periodic audits of Customer's use of MVR Data. Further, in response to any audit, Customer must be able to substantiate the reasonfor each MVR Data order.

(x) **American Board of Medical Specialties ("ABMS") Data.** If Customer is permitted to access ABMS Data from Credit Technologies Inc., Customer shall not use , nor permit others to use, ABMS Data for purposes of determining, monitoring, tracking, profiling or evaluating in any manner the patterns or frequency of physicians' prescriptions or medications, pharmaceuticals, controlled substances, or medical devices for use by their patients.

(xi) **HIPAA**. Customer represents and warrants that Customer will not provide Credit Technologies Inc. with any Protected Health Information (as that term is defined in 45 C.F.R. Sec. 160.103) or with Electronic Health Records or Patient Health Records (as those terms are defined in 42 U.S.C. Sec. 17921(5), and 42 U.S.C. Sec. 17921(11), respectively) or with information from such records without the execution of a separate agreement between the parties.

(xii) **Retention of Records.** For uses of GLB Data, DPPA Data and MVR Data, as described in Sections 1(ii), 1(iii) and 1(ix), Customer shall maintain for a period of five (5) years a complete and accurate record (including consumer identity, purpose and, if applicable, consumer authorization) pertaining to every access to such data.

(xiii) **Economic Sanctions Laws.** Customer acknowledges that Credit Technologies Inc. is subject to economic sanctions laws, including but not limited to those enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the European Union, and the United Kingdom. Accordingly, Customer shall comply with all economic sanctions laws of the United States, the European Union, and the United Kingdom. Customer shall not provide access to Credit Technologies Inc. Services to any individuals identified on OFAC's list of Specially Designated Nationals ("SDN List"), the UK's HM Treasury's Consolidated List of Sanctions Targets, or the EU's Consolidated List of Persons, Groups, and Entities Subject to EU Financial Sanctions. Customer shall not take any action, which would place Credit Technologies Inc. in a position of non-compliance with any such economic sanctions laws.

2. SECURITY. Customer acknowledges that the information available through the Credit Technologies Inc. Services may include personally identifiable information and it is Customer's obligation to keep all such accessed information confidential and secure. Accordingly, Customer shall:

(a) restrict access to Credit Technologies Inc. Services to those employees who have a need to know as part of their official duties;

(b) ensure that none of its employees shall:

(i) obtain and/or use any information from the Credit Technologies Inc. Services for personal reasons, or

(ii) transfer any information received through the Credit Technologies Inc. Services to any party except as permitted hereunder;

(c) keep all user identification numbers, and related passwords, or other security measures (collectively, "User IDs") confidential and prohibit the sharing of User IDs;

(d) immediately deactivate the User ID of any employee who no longer has a need to know, or for terminated employees on or prior to the date of termination;

(e) in addition to any obligations under Paragraph 1, take all commercially reasonable measures to prevent unauthorized access to, or use of, the Credit Technologies Inc. Services or data received therefrom, whether the same is in electronic form or hard copy, by any person or entity;

(f) maintain and enforce data destruction procedures to protect the security and confidentiality of all information obtained through Credit Technologies Inc. Services as it is being disposed;

(g) unless otherwise required by law, purge all information received through the Credit Technologies Inc. Services and stored electronically or on hard copy by Customer within ninety (90) days of initial receipt;

(h) be capable of receiving the Credit Technologies Inc. Services where the same are provided utilizing "secure socket layer," or such other means of secure transmission as is deemed reasonable by Credit Technologies Inc.;

(i) not access and/or use the Credit Technologies Inc. Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by Credit Technologies Inc.; and

(j) take all steps to protect their networks and computer environments, or those used to access the Credit Technologies Inc. Services, from compromise.

Customer agrees that on at least a quarterly basis it will review searches performed by its User IDs to ensure that such searches were performed for a legitimate business purpose and in compliance with all terms and conditions herein. Customer will implement policies and procedures to prevent unauthorized use of User IDs and the Credit Technologies Inc. Services and will immediately notify Credit Technologies Inc., in writing to the Credit Technologies Inc. if Customer suspects, has reason to believe or confirms that a User ID or the Credit Technologies Inc. Services (or data derived directly or indirectly therefrom) is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose other than legitimate business reasons. Customer shall remain solely liable for all costs associated therewith and shall further reimburse Credit Technologies Inc. for any expenses it incurs due to Customer's failure to prevent such impermissible use or access of User IDs and/or the Credit Technologies Inc. Services, or any actions required as a result thereof. Furthermore, in the event that the Credit Technologies Inc. Services provided to the Customer include personally identifiable information (including, but not limited to, social security numbers, driver's license numbers or dates of birth), the following shall apply: Customer acknowledges that, upon unauthorized acquisition or access of or to such personally identifiable information, including but not limited to that which is due to use by an unauthorized person or due to unauthorized use (a "Security Event"), Customer shall, in compliance with law, notify the individuals whose information was potentially accessed or acquired that a Security Event has occurred, and shall also notify any other parties (including but not limited to regulatory entities and credit reporting agencies) as may be required in Credit Technologies Inc.'s reasonable discretion. Customer agrees that such notification shall not reference Credit Technologies Inc. or the product through which the data was provided, nor shall Credit Technologies Inc. be otherwise identified or referenced in connection with the Security Event, without Credit Technologies Inc.'s express written consent. Customer shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Security Event and shall bear all costs associated with complying with legal and regulatory obligations in connection therewith. Customer shall remain solely liable for claims that may arise from a Security Event, including, but not limited to, costs for litigation (including attorneys' fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Security Event, and to the extent that any claims are brought against Credit Technologies Inc., shall indemnify Credit Technologies Inc. from such claims. Customer shall provide samples of all proposed materials to notify consumers and any third- parties, including regulatory entities, to Credit Technologies Inc. for review and approval prior to distribution. In the event of a Security Event, Credit Technologies Inc. may, in its sole discretion, take immediate action, including suspension or termination of Customer's account, without further obligation or liability of any kind.

3. PERFORMANCE. Credit Technologies Inc. will use commercially reasonable efforts to deliver the Credit Technologies Inc. Services requested by Customer and to compile information gathered from selected public records and other sources used in the provision of the Credit Technologies Inc. Services; provided, however, that Customer accepts all information "**AS IS**." Customer acknowledges and agrees that Credit Technologies Inc. obtains its data from third-party sources, which may or may not be completely thorough and accurate, and that Customer shall not rely on Credit Technologies Inc. for the accuracy or completeness of information supplied through the Credit Technologies Inc. Services. Without limiting the foregoing, the criminal record data that may be provided as part of the Credit Technologies Inc. Services may include records that have been expunged, sealed, or otherwise have become inaccessible to the public since the date on which the data was last updated or collected. Customer understands that Customer may be restricted from accessing certain Credit Technologies Inc. Services, which may be otherwise available. Credit Technologies Inc. reserves the right to add materials and features to, and to discontinue offering any of the materials and features that are currently a part of, the Credit Technologies Inc. Services. In the event that Credit Technologies Inc. discontinues a material portion of the materials and features that Customer regularly uses in the ordinary course of its business, and such materials and features are part of a flat fee subscription plan to which Customer has subscribed, Credit Technologies Inc. will, at Customer's option, issue a prorated credit to Customer's account.

4. INTELLECTUAL PROPERTY; CONFIDENTIALITY. Customer agrees that Customer shall not reproduce, retransmit, republish, or otherwise transfer for any commercial purposes the Credit Technologies Inc. Services' information, programs or computer applications. Customer acknowledges that Credit Technologies Inc. (and/or its third party data providers) shall retain all right, title, and interest under applicable contractual, copyright, patent, trademark, Trade Secret and related laws in and to the Credit Technologies Inc. Services and the data and information that they provide. Customer shall use such materials in a manner consistent with Credit Technologies Inc.'s interests and the terms and conditions herein, and shall notify Credit Technologies Inc. of

any threatened or actual infringement of Credit Technologies Inc.'s rights. Notwithstanding anything in this Agreement to the contrary, Credit Technologies Inc. or Credit Technologies Inc.'s data provider shall own Customer's search inquiry data used to access the Credit Technologies Inc. Services (in the past or future) and may use such data for any purpose consistent with applicable federal, state and local laws, rules and regulations. Customer and Credit Technologies Inc. acknowledge that they each may have access to confidential information of the disclosing party ("Disclosing Party") relating to the Disclosing Party's business including, without limitation, technical, financial, strategies and related information, computer programs, algorithms, know-how, processes, ideas, inventions (whether patentable or not), schematics, Trade Secrets (as defined below) and other information (whether written or oral), and in the case of Credit Technologies Inc.'s information, product information, pricing information, product development plans, forecasts, data contained in Credit Technologies Inc. Services, and other business information ("Confidential Information"). Confidential Information shall not include information that:

(i) is or becomes (through no improper action or inaction by the Receiving Party (as defined below)) generally known to the public;

(ii) was in the Receiving Party's possession or known by it prior to receipt from the Disclosing Party;

(iii) was lawfully disclosed to Receiving Party by a third-party and received in good faith and without any duty of confidentiality by the Receiving Party or the third-party; or

(iv) was independently developed without use of any Confidential Information of the Disclosing Party by employees of the Receiving Party who have had no access to such Confidential Information.

"Trade Secret" shall be deemed to include any information which gives the Disclosing Party an advantage over competitors who do not have access to such information as well as all information that fits the definition of "trade secret" set forth in the Official Code of Georgia Annotated § 10-1-761(4). Each receiving party ("Receiving Party") agrees not to divulge any Confidential Information or information derived therefrom to any third-party and shall protect the confidentiality of the Confidential Information with the same degree of care it uses to protect the confidentiality of its own confidential information and trade secrets, but in no event less than a reasonable degree of care. Notwithstanding the foregoing, the Receiving Party may disclose Confidential Information solely to the extent required by subpoena, court order or other governmental authority, provided that the Receiving Party shall give the Disclosing party prompt written notice of such subpoena, court order or other governmental authority so as to allow the Disclosing party to have an opportunity to obtain a protective order to prohibit or restrict such disclosure at its sole cost and expense. Confidential Information disclosed pursuant to subpoena, court order or other governmental authority shall otherwise remain subject to the terms applicable to Confidential Information. Each party's obligations with respect to Confidential Information shall continue for the term of this Agreement and for a period of five (5) years thereafter, provided however, that with respect Trade Secrets, each party's obligations shall continue for so long as such Confidential Information continues to constitute a Trade Secret.

5. WARRANTIES/LIMITATION OF LIABILITY. Neither Credit Technologies Inc., nor its subsidiaries and affiliates, nor any third- party data provider (for purposes of indemnification, warranties, and limitations on liability, Credit Technologies Inc., its subsidiaries and affiliates, and its data providers are hereby collectively referred to as "Credit Technologies Inc.") shall be liable to Customer (or to any person claiming through Customer to whom Customer may have provided data from the Credit Technologies Inc. Services) for any loss or injury arising out of or caused in whole or in part by Credit Technologies Inc.'s acts or omissions in procuring, compiling, collecting, interpreting, reporting, communicating, or delivering the Credit Technologies Inc. Services. If, notwithstanding the foregoing, liability can be imposed on Credit Technologies Inc., then Customer agrees that Credit Technologies Inc.'s aggregate liability for any and all losses or injuries arising out of any act or omission of Credit Technologies Inc. in connection with anything to be done or furnished under this Agreement, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed One Hundred Dollars ($100.00); and Customer covenants and promises that it will not sue Credit Technologies Inc. for an amount greater than such sum even if Customer and/or third parties were advised of the possibility of such damages and that it will not seek punitive damages in any suit against Credit Technologies Inc. Credit Technologies Inc. does not make and hereby disclaims any warranty, express or implied with respect to the Credit Technologies Inc. Services.

Credit Technologies Inc. does not guarantee or warrant the correctness, completeness, merchantability, or fitness for a particular purpose of the Credit Technologies Inc. Services or information provided therein. In no event shall Credit Technologies Inc. be liable for any indirect, incidental, or consequential damages, however arising, incurred by Customer from receipt or use of information delivered hereunder or the unavailability thereof. Due to the nature of public record information, the public records and commercially available data sources used in Credit Technologies Inc. Services may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. Credit Technologies Inc. Services are not the source of data, nor are they a comprehensive compilation of the data. Before relying on any data, it should be independently verified.

6. INDEMNIFICATION. Customer hereby agrees to protect, indemnify, defend, and hold harmless Credit Technologies Inc. from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or inany way related to:

(a) use of information received by Customer (or any third party receiving such information from or through Customer) furnished by or through Credit Technologies Inc.;

(b) breach of any terms, conditions, representations or certifications in this Agreement; and

(c) any Security Event.

Credit Technologies Inc. hereby agrees to protect, indemnify, defend, and hold harmless Customer from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in connection with any third-party claim that the [RESELLER] Services or data contained therein, when used in accordance with this Agreement, infringe a United States patent or United States registered copyright, subject to the following:

(xiv) Customer must promptly give written notice of any claim to Credit Technologies Inc.;

(xv) Customer must provide any assistance which Credit Technologies Inc. may reasonably request for the defense of the claim (with reasonable out of pocket expenses paid by Credit Technologies Inc.); and

(xvi) Credit Technologies Inc. has the right to control the defense or settlement of the claim; provided, however, that the Customer shall have the right to participate in, but not control, any litigation for which indemnification is sought with counsel of its own choosing, at its own expense.

Notwithstanding the foregoing, Credit Technologies Inc. will not have any duty to indemnify, defend or hold harmless Customer with respect to any claim of infringement resulting from:

(1) Customer's misuse of the Credit Technologies Inc. Services;
(2) Customer's failure to use any corrections made available by Credit Technologies Inc.;
(3) Customer's use of the Credit Technologies Inc. Services in combination with any product or information not provided or authorized in writing by Credit Technologies Inc.; or
(4) any information, direction, specification or materials provided by Customer or any third-party.

If an injunction or order is issued restricting the use or distribution of any part of the Credit Technologies Inc. Services, or if Credit Technologies Inc. determines that any part of the Credit Technologies Inc. Services is likely to become the subject of a claim of infringement or violation of any proprietary right of any third-party, Credit Technologies Inc. may in its sole discretion and at its option:

(A) procure for Customer the right to continue using the Credit Technologies Inc. Services;

(B) replace or modify the Credit Technologies Inc. Services so that they become non-infringing, provided such modification or replacement does not materially alter or affect the use or operation of the Credit Technologies Inc. Services; or

(C) terminate this Agreement and refund any fees relating to the future use of the Credit Technologies Inc. Services. The foregoing remedies constitute Customer's sole and exclusive remedies and Credit Technologies Inc.'s entire liability with respect to infringement claims or actions.

7. AUDIT. Customer understands and agrees that, in order to ensure compliance with the FCRA, GLBA, DPPA, other similar state or federal laws, regulations or rules, regulatory agency requirements, this Agreement, and Credit Technologies Inc.'s obligations under its contracts with its data providers and Credit Technologies Inc.'s internal policies, Credit Technologies Inc. may conduct periodic reviews of Customer's use of the Credit Technologies Inc. Services and may, upon reasonable notice, audit Customer's records, processes and procedures related to Customer's use, storage and disposal of Credit Technologies Inc. Services and information received therefrom. Customer agrees to cooperate fully with any and all audits and to respond to any such audit inquiry within ten (10) business days, unless an expedited response is required. Violations discovered in any review and/or audit by Credit Technologies Inc. will be subject to immediate action including, but not limited to, suspension or termination of the license to use the Credit Technologies Inc. Services, reactivation fees, legal action, and/or referral to federal or state regulatory agencies.

8. SURVIVAL OF AGREEMENT. Provisions hereof related to release of claims; indemnification; use and protection of information, data and Credit Technologies Inc. Services; payment for the Credit Technologies Inc. Services; audit; Credit Technologies Inc.'s use and ownership of Customer's search inquiry data; disclaimer of warranties; security; customer data and governing law shall survive any termination of the license to use the Credit Technologies Inc. Services.

9. EMPLOYEE TRAINING. Customer shall train new employees prior to allowing access to Credit Technologies Inc. Services on Customer's obligations under this Agreement, including, but not limited to, the licensing requirements and restrictions under Paragraph 1 and the security requirements of Paragraph 2. Customer shall conduct a similar review of its obligations under this Agreement with existing employees who have access to Credit Technologies Inc. Services no less than annually. Customer shall keep records of such training.

10. ATTORNEYS' FEES. The prevailing party in any action, claim or lawsuit brought pursuant to this Agreement is entitled to payment of all attorneys' fees and costs expended by such prevailing party in association with such action, claim or lawsuit.

11. TAXES. The charges for all Credit Technologies Inc. Services are exclusive of any state, local, or otherwise applicable sales, use, or similar taxes. If any such taxes are applicable, they shall be charged to Customer's account.

12. CUSTOMER CHANGES/CREDIT REPORT. Customer acknowledges and understands that Credit Technologies Inc. will only allow Customer access to the Credit Technologies Inc. Services if Customer's credentials can be verified in accordance with Credit Technologies Inc.'s internal credentialing procedures. Customer shall notify Credit Technologies Inc. immediately of any changes to the information on Customer's Application for the Credit Technologies Inc. Services, and, if at any time Customer no longer meets Credit Technologies Inc.'s criteria for providing such service, Credit Technologies Inc. may terminate this Agreement. Customer is required to promptly notify Credit Technologies Inc. of a change in ownership of Customer's company, any change in the name of Customer's company, and/or any change in the physical address of Customer's company.

13. RELATIONSHIP OF PARTIES. None of the parties shall, at any time, represent that it is the authorized agent or representative of the other.

14. CHANGE IN AGREEMENT. By receipt of the Credit Technologies Inc. Services, Customer agrees to, and shall comply with, changes to the Restricted License granted Customer in Paragraph 1 herein, changes in pricing, and changes to other provisions of this Agreement as Credit Technologies Inc. shall make from time to time by notice to Customer via e-mail, online "click wrap" amendments, facsimile, mail, invoice announcements, or other written notification. All e-mail notifications shall be sent to the individual named in the Customer Administrator Contact Information section, unless stated otherwise in this Agreement. Credit Technologies Inc. may, at any time, impose restrictions and/or prohibitions on the Customer's use of the Credit Technologies Inc. Services or certain data. Customer understands that such restrictions or changes in access may be the result of a modification in Credit Technologies Inc. policy, a modification of third-party agreements, a modification in industry standards, a Security Event or a change in law or regulation, or the interpretation thereof. Upon written notification by Credit Technologies Inc. of such restrictions, Customer agrees to comply with such restrictions.

15. PUBLICITY. Customer will not name Credit Technologies Inc. or refer to its use of the Credit Technologies Inc. Services in any press releases, advertisements, promotional or marketing materials, or make any other third-party disclosures regarding Credit Technologies Inc. or Customer's use of the Credit Technologies Inc. Services.

16. FORCE MAJEURE. The parties will not incur any liability to each other or to any other party on account of any loss or damage resulting from any delay or failure to perform all or any part of this Agreement (except for payment obligations) to the extent such delay or failure is caused, in whole or in part, by events, occurrences, or causes beyond the control, and without the negligence of, the parties. Such events, occurrences, or causes include, without limitation, acts of God, telecommunications outages, Internet outages, power outages, any irregularity in the announcing or posting of updated data files by the applicable agency, strikes, lockouts, riots, acts of war, floods, earthquakes, fires, and explosions.

17. PRIVACY PRINCIPLES. With respect to personally identifiable information regarding consumers, the parties further agree as follows: Credit Technologies Inc. has adopted the "Credit Technologies Inc. Data Privacy Principles" ("Principles"), which may be modified from time to time, recognizing the importance of appropriate privacy protections for consumer data, and Customer agrees that Customer (including its directors, officers, employees or agents) will comply with the Principles or Customer's own comparable privacy principles, policies, or practices. The Principles are available at: http://www.credittechnologies.com/.

18. ENTIRE AGREEMENT. Except as otherwise provided herein, this Agreement constitutes the final written agreement and understanding of the parties and is intended as a complete and exclusive statement of the terms of the agreement, which shall supersede all other representations, agreements, and understandings, whether oral or written, which relate to the use of the Credit Technologies Inc. Services and all matters within the scope of this Agreement. Without limiting the foregoing, the provisions related to confidentiality and exchange of information contained in this Agreement shall, with respect to the Credit Technologies Inc. Services and all matters within the scope of this Agreement, supersede any separate non-disclosure agreement that is or may in the future be entered into by the parties hereto. Any new, other, or different terms supplied by the Customer beyond the terms contained herein, including those contained in purchase orders or confirmations issued by the Customer, are specifically and expressly rejected by Credit Technologies Inc. unless Credit Technologies Inc. agrees to them in a signed writing specifically

including those new, other, or different terms. The terms contained herein shall supersede and govern in the event of a conflict between these terms and any new, other, or different terms in any other writing. This Agreement can be executed in counterparts and faxed or electronic signatures will be deemed originals.

19. MISCELLANEOUS. If any provision of this Agreement or any exhibit shall be held by a court of competent jurisdiction to be contrary to law, invalid or otherwise unenforceable, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law, and in any event the remaining provisions of this Agreement shall remain in full force and effect. The headings in this Agreement are inserted for reference and convenience only and shall not enter into the interpretation hereof.

Exhibit F

VERMONT STATUTE

Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999) § 2480e. Consumer consent

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

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

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

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

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

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

(2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

VERMONT RULES *** CURRENT THROUGH JUNE 1999 ***
AGENCY 06. OFFICE OF THE ATTORNEY GENERAL SUB •AGENCY 031. CONSUMER PROTECTION DIVISION CHAPTER 012. Consumer Fraud ••Fair Credit Reporting
RULE CF 112 FAIR CREDIT REPORTING CVR 06 •031 •012, CF 112.03 (1999) CF 112.03 CONSUMER CONSENT

(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 9V.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.

Exhibit G

CALIFORNIA END USER

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

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

Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver 's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

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

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed." In compliance with Section 1785.14(a) of the California Civil Code, End User hereby certifies to Consumer Reporting Agency as follows:

End User is not a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller ") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale ").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

End User also certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

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

Exhibit H

DISPOSAL OF CONSUMER INFORMATION

As used herein, the term "Consumer Information" shall mean any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer Information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

"Dispose, "disposing," or "disposal" means:

(1) the discarding or abandonment of consumer information; or,

(2) the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.

Proper Disposal of Consumer Information

(a) Standard. Any person who maintains Consumer Information for a business purpose must properly dispose ofsuch information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(b) Examples. Reasonable measures to protect against unauthorized access to or use of Consumer Information in connection with its disposal include the following examples:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule.

(4) For persons who maintain consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (b)(1) and (2) of this section.