Exhibit A

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

NOTICE TO USERS OF CONSUMER REPORTS:

OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Bureau of Consumer Financial Protection's website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Bureau's website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.** The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a) (2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a) (3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a) (3)(F) (i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a) (3)(F) (ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section604(a) (3) (D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section604(a)(3)(E)

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

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

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

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

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

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

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed, which will be issued by the Consumer Financial Protection Bureau and the banking and credit union regulators.

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

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The Consumer Financial Protection Bureau, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Consumer Financial Protection Bureau regulations may be found at www.consumerfinance.gov/learnmore.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

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

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.

- Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

  In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2).

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

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

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(1), 604(c), 604(e), and 614(d). This practice is known as "prescreening" and typically involves obtaining a list of consumers from a CRA who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must:

1) before the offer is made, establish the criteria that will be relied upon to make the offer and grant credit or insurance, and

2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

   - Information contained in a consumer's CRA file was used in connection with the transaction.
   - The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
   - Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral. The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

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

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  1. the identify of all end-users;
  2. certifications from all users of each purpose for which reports will be used; and
  3. certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

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

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1618 et seq.:

	15 U.S.C. 1681
Section 603	15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605 A	15 U.S.C. 1681c-1
Section 605 B	15 U.S.C. 1681c-2
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 612	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 16811
Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 16810
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 168H
Section 621	15 U.S.C. 1681s
Section 622	15 U.S.C. 16815-1
Section 623	15 U.S.C. 16815-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y

Exhibit B

EQUIFAX
REQUIRMENTS

Customer, in order to receive consumer credit information from Equifax Information Services, LLC, through CTI agrees to comply with the following conditions required by Equifax, which may be in addition to those outlined in the Customer Service Agreement ("Agreement"). Customer understands and agrees that Equifax'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 Equifax consumer credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

1. Customer hereby agrees to comply with all current and future policies and procedures instituted by CTI and required by Equifax. 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.

2. Customer certifies that it will order and use Limited-ID or Limited DTEC reports in connection with only one of the following purposes involving the subject of the report and for no other purpose:

   (a) to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;

   (b) for required institutional risk control or for resolving consumer disputes or inquiries;

   (c) due to holding a legal or beneficial interest relating to the consumer;

   (d) as necessary to effect, administer, or enforce a transaction to underwrite insurance at the consumer's request, for reinsurance purposes or for the following purposes related to the consumer's insurance: account administration, reporting, investigation fraud prevention, premium payment processing, claim processing, benefit administration or research projects;

   (e) to persons acting in a fiduciary or representative capacity on behalf of, and with the consent of, the consumer or

   (f) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, including location for collection of a delinquent account. Customer, if a government agency, certifies it will order and use Limited-ID or Limited DTEC in connection with the following purposes involving the subject and for no other purpose:

      a. pursuant to FCRA Section 608 or

      b. for an investigation on a matter related to public safety. Equifax may periodically conduct audits of Customer regarding its compliance with the FCRA and other certifications in this Agreement.

   Audits will be conducted by mail whenever possible and will require Customers to provide documentation as to permissible use of particular consumer, Limited ID, or Limited DTEC reports. Customer gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Customer's material breach of this Agreement, constitute grounds for immediate suspension of service or, termination of this Agreement notwithstanding Paragraph 6 above. If Equifax terminates this Agreement due to the conditions in the preceding sentence, Customer

      (i) unconditionally releases and agrees to hold EQUIFAX harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and

      (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

3. 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 Equifax.

4. Customer agrees that Equifax shall have the right to audit records of Customer that are relevant to the provision of services set forth in this agreement. Customer authorizes CTI to provide to Equifax, upon Equifax'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 Equifax regarding Equifax information. Customer understands that Equifax may require CTI to suspend or terminate access to Equifax'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.

5. Equifax information will be requested only for Customer's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted by law. Customer agrees that Equifax information will not be forwarded or shared with any third party unless required by law or approved by Equifax. If approved by Equifax 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 Equifax may charge a fee for the subsequent delivery to secondary users. Only designated representatives of Customer will request Equifax information on Customer's employees, and employees will be forbidden to obtain reports on themselves, associates or any other persons except in the exercise of their official duties. Customer will not disclose Equifax information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax. Customer will hold Equifax and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax information by Customer, its employees or agents contrary to the conditions of this paragraph or applicable law.

6. Customer understands that it must meet the following criteria:

   (a) the Customer company name, including any DBA's, and the address on the Customer Application ("Application") and Agreement must match;

   (b) the telephone listing must be verified in the same company name and address that was provided on the Application and Agreement;

   (c) a copy of the current lease of the business must be reviewed by CTI to confirm the Customer is at the same address that is shown on the Application and Agreement, and the following pages of the lease

   (d) must be reviewed for verification: the signature page; the address page; the terms of the lease page; landlord name and landlord contact information;

   (e) a copy of the principal's driver's license is required to verify the principal's identity;

   (f) a current business license must be supplied, and reflect the same name and at the same address provided on the Application and Agreement. (Contact CTI for valid substitutions when a license is not required by the state), and

   (g) an on-site inspection of the office is to be conducted by an Equifax certified company.

   **Note (c) and (d) are not required if the Customer is publicly traded on a nationally recognized stock exchange.*

7. Customer will be charged for Equifax consumer credit information by CTI, which is responsible for paying Equifax for such information; however, should the underlying relationship between CTI and Customer terminate at any time during this agreement, charges for Equifax consumer credit information will be invoiced to Customer, and Customer will be solely responsible to pay Equifax directly.

8. Customer agrees that it will properly dispose of all consumer information in accordance with the following. As used herein, "consumer information" means 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. A Customer who maintains consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

a. Reasonable measures include

i. 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;

ii. 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; and

iii. 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 the above.

9. Customer agrees to hold harmless Equifax and its directors, officers, employees, agents, successors and assigns, from and against any and all liabilities, claims, losses, demands, actions, causes of action, damages, expenses (including, without limitation, attorney's fees and costs of litigation), or liability, arising from or in any manner related to any allegation, claim, demand or suit, whether or not meritorious, brought or asserted by any third party arising out of or resulting from any actual or alleged negligence or intentional act of Customer, whether or not any negligence of Equifax is alleged to have been contributory thereto, the failure of Customer to misuse or improper access to Equifax consumer credit information by Customer or the failure of Customer to comply with applicable laws or regulations. Customer further understands and agrees that the accuracy of any consumer credit information is not guaranteed by Equifax and releases Equifax from liability for any loss, cost, expense or damage, including attorney's fees, suffered by Customer resulting directly or indirectly from its use of consumer credit information from Equifax.

10. EQUIFAX MAKES NO REPRESENTATIONS, WARRANTIES, OR GUARANTEES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, RESPECTING ACROPACORANY OTHER MACHINERY, EQUIPMENT, MATERIALS, PROGRAMMING AIDS OR OTHER ITEMS UTILIZED BY CUSTOMER IN CONNECTION WITH OR RELATED TO, OR RESPECTING THE ACCURACY OF, ANY EQUIFAX CREDIT INFORMATION FURNISHED BY EQUIFAX TO ANY CUSTOMER.

11. Fair Credit Reporting Act Certification. Customer certifies that it will order Equifax Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Customer intends to use that consumer report information:

(a) in accordance with the FCRA and all state law counterparts; and

(b) for one of the following permissible purposes:

(i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer;

(ii) in connection with the underwriting of insurance involving the consumer;

(iii) as a potential investor or services, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation;

(iv) when Customer otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer, or to review an account to determine whether the consumer continues to meet the terms of the accounts; or

(v) for employment purposes; provided, however, that CUSTOMER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYEMENT PURPOSES UNLESS CUSTOMER HAS A SUBCRIPTION TC THE EQUIFAX PERSONA SERVICE.

Customer will use each consumer report ordered under this Agreement for one of the foregoing purposes and for no other purpose. It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency (such as Equifax) under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Customer regarding its compliance with the FCRA and other certifications in this Agreement. Audits will be conducted by mail whenever possible and will require Customers to provide documentation as to permissible use of particular consumer, Limited ID, or Limited DTEC reports. Customer gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Customer's material breach of this Agreement, constitute grounds for immediate suspension of service or, termination of this Agreement notwithstanding Paragraph 6 above. If Equifax terminates this Agreement due to the conditions in the preceding sentence, Customer:

(i) unconditionally releases and agrees to hold EQUIFAX harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and

(ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination. California Law Certification. Customer will refer to Exhibit 1-A in making the following certification, and Customer agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.

Customer certifies that it IS NOT a "retail seller," as defined in Section 1802.3 of the California Civil Code and DOES NOT issue credit to consumers who appear in person on the basis of an application for credit submitted in person.

Vermont Certification. Customer certifies that it will comply with applicable provisions under Vermont law. In particular, Customer certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after Customer has received prior consumer consent in accordance with VFCRA Section 248oe and applicable Vermont Rules. Customer further certifies that the attached copy of Section 248oe (Exhibit 1-B) of the Vermont Fair Credit Reporting Statute was received from EQUIFAX.

Customer will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act, Gramm-Leach- Bliley Act and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer. 12. This Section 12 applies to any means through which Customer orders or accesses the Information Services including, without limitation, system-to-system, direct access terminal, personal computer or the Internet; provided, however, Customer will not order or access the Information Services via the Internet without first obtaining Equifax's written permission. For the purposes of this Section 9, the term "Authorized User" means a Customer employee that Customer has authorized to order or access the Information Services and who is trained on Customer's obligations under this Agreement with respect to the ordering and use of the Information Services, and the information provided through same, including Customer's FCRA and other obligations with respect to the access and use of consumer reports.

Customer will:

(a) ensure that only Authorized Users can order or have access to the Information Services and the information provided through same,

(b) ensure that Authorized Users do not order credit reports for personal reasons or provide them to any third party,

(c) ensure that all devices used by Customer to order or access the Information Services are placed in a secure location and accessible only by Authorized Users and that these devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures, and

(d) take all necessary measures to prevent unauthorized ordering or access to the Information Services by any persons other than Authorized Users for permissible purposes.

Those measures will include, without limitation, limiting the knowledge of the Customer security codes, telephone access number(s) Equifax provides, and any passwords Customer may use, to Authorized Users and other employees with a need to know, changing Customer's user passwords at least every ninety (90) days, or sooner if it is obtained by any third party or an Authorized User is no longer responsible for accessing the Information Services, or if Customer suspects an unauthorized person has learned the password, and using all security features in the software and hardware Customer uses to order or access the Information Services.

Customer will monitor compliance with the obligations of this Section 12, and will immediately notify Equifax if Customer suspects or knows of any unauthorized access or attempt to access the Information Services. Such monitoring will include, without limitation, a review of each Equifax invoice for the purpose of detecting any unauthorized activity.

Customer will not ship hardware or software between Customer's locations or to third parties without deleting all Equifax Customer number(s), security codes, telephone access number(s) and Customer user passwords. If Customer uses a third-party vendor to establish access to the Information Services, Customer is responsible for the third-party vendor's use of Customer's member numbers, security access codes, or passwords. Customer will ensure the third-party vendor safeguards Customer's security access code(s) and passwords through the use of security requirements that are no less stringent than those applicable to Customer under this Section 9.

Customer will inform Authorized Users and other employees with a need to know that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment. If Equifax reasonably believes that Customer has violated this Section 12, Equifax may, in addition to any other remedy authorized by this Agreement, with reasonable advance written notice to Customer and at Equifax's sole expense, conduct, or have a third party conduct on its behalf, an audit of Customer's network security systems, facilities, practices and procedures to the extent Equifax reasonably deems necessary in order to evaluate Customer's compliance with the data security requirements of this Section 12.

Exhibit C

EXPERIAN
REQUIRMENTS

Customer, in order to receive consumer credit information from Experian Information Solutions, Inc, agrees to comply with the following conditions required by Experian, which may be in addition to those outlined in the Customer Service Agreement ("Agreement"), of which these conditions are made a part. Customer understands and agrees that Experian'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 Experian credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

1. Customer hereby agrees to comply with all current and future policies and procedures instituted by CTI and required by Experian. 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.

2. Customer agrees that Experian shall have the right to audit records of Customer that are relevant to the provision of services set forth in this Agreement and to verify, through audit or otherwise, that Customer is in compliance with applicable law and the provisions of this Agreement and is fact the end user of the credit information with no intention to resell or otherwise provide or transfer the credit information in whole or in part to any other person or entity. Customer authorizes CTI to provide to Experian, upon Experian's request, all materials and information relating to its investigations of Customer. Customer further agrees that it will respond within the requested time frame indicated for information requested by Experian regarding Experian consumer credit information. Customer understands that Experian may require CTI to suspend or terminate access to Experian information in the event Customer does not cooperate with any such an investigation or in the event Customer is not in compliance with applicable law or this Agreement. Customer shall remain responsible for the payment for any services provided to Customer by CTI prior to any such discontinuance.

3. Customer certifies that it is not a reseller of the information, a private detective agency, 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, asset location service, a company engaged in selling future services (health clubs, etc.), news agency, business that operates out of an apartment or a residence, 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 Experian. Customer further certifies that Experian data may only be used for the permissible purpose stated in the agreement, and any/all fraud products will only be used to protect against fraud.

4. Customer agrees that it will maintain proper access security procedures consistent with industry standards and that if a data breach occurs or is suspected to have occurred in which Experian information is compromised or is potentially compromised, Customer will take the following action:

    (a) Customer will notify CTI within 24 hours of a discovery of a breach of the security of consumer reporting data if the personal information of consumers was, or is reasonably believed to have been, acquired by an unauthorized person. Further, Customer will actively cooperate with and participate in any investigation conducted by CTI or Experian that results from Customer's breach of Experian consumer credit information.

    (b) In the event that Experian determines that the breach was within the control of Customer, Customer will provide notification to affected consumers that their personally sensitive information has been or may have been com promised. Experian will have control over the nature and timing of the consumer correspondence related to the breach when Experian information is involved.

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

credit reporting bureau.

(d) Customer understands and agrees that if the root cause of the breach is determined by Experian to be under the 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 Security Requirements

The security requirements included in this document represent the minimum-security requirements acceptable to Experian and are intended to ensure that a Third Party (i.e., Supplier, Reseller, Service Provider or any other organization engaging with Experian) has appropriate controls in place to protect information and systems, including any information that it receives, processes, transfers, transmits, stores, delivers, and / or otherwise accesses on behalf of Experian.

DEFINITIONS

"Experian Information" means Experian highly sensitive information including, by way of example and not limitation, data, databases, application software, software documentation, supporting process documents, operation process and procedures documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, financial records, employee records, and information about potential acquisitions, and such other information that is similar in nature or as mutually agreed in writing, the disclosure, alteration or destruction of which would cause serious damage to Experian's reputation, valuation, and / or provide a competitive disadvantage to Experian.

"Resource" means all Third-Party devices, including but not limited to laptops, PCs, routers, servers, and other computer systems that store, process, transfer, transmit, deliver, or otherwise access the Experian Information.

1. **Information Security Policies and Governance**
   Third Party shall have Information Security policies and procedures in place that are consistent with the practices described in an industry standard, such as ISO 27002 and / or this Security Requirements document, which is aligned to Experian's Information Security policy.

2. **Vulnerability Management**
   Firewalls, routers, servers, PCs, and all other resources managed by Third Party (including physical, on-premise or cloud hosted infrastructure) will be kept current with appropriate security specific system patches. Third Party will perform regular penetration tests to further assess the security of systems and resources. Third Party will use end-point computer malware detection / scanning services and procedures.

3. **Logging and Monitoring**
   Logging mechanisms will be in place sufficient to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted, or locked) with a process for periodic review.

4. **Network Security**
   Third Party will use security measures, including anti-virus software, to protect communications systems and networks device to reduce the risk of infiltration, hacking, access penetration by, or exposure to, an unauthorized third-party.

5. **Data Security**
   Third Party will use security measures, including encryption, to protect Experian provided data in storage and in transit to reduce the risk of exposure to unauthorized parties

6. **Remote Access Connection Authorization**
   All remote access connections to Third Party internal networks and / or computer systems will require authorization with access control at the point of entry using multi-factor authentication. Such access will use secure channels, such as a Virtual Private Network (VPN).

7. **Incident Response**
   Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents. Third Party will report actual or suspected security violations or incidents that may affect Experian to Experian within twenty-four (24) hours of Third Party's confirmation of such violation or incident.

8. **Identification, Authentication and Authorization**
   Each user of any Resource will have a uniquely assigned user ID to enable individual authentication and accountability. Access to privileged accounts will be restricted to those people who administer the Resource and individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.

9. **User Passwords and Accounts**
   All passwords will remain confidential and use 'strong' passwords that expire after a maximum of 90 calendar days. Accounts will automatically lockout after five (5) consecutive failed login attempts.

10. **Training and Awareness**
    Third Party shall require all Third-Party personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel.

11. **Experian's Right to Audit**
    Third Party shall be subject to remote and / or onsite assessments of its information security controls and compliance with these Security Requirements.

12. **Bulk Email Communications into Experian**
    Third party will not "bulk email" communications to multiple Experian employees without the prior written approval of Experian. Third party shall seek authorization via their Experian Relationship Owner in advance of any such campaign.

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

TRANSUNION
REQUIRMENTS

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 its 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 deliverthe 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 WARRAN1Y SET FORTH INTHE PREVIOUS SENTENCE IS THE SOLE WARRAN1Y 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 WARRAN1Y 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 MERCHANTABILl1Y OR FITNESS FOR A PARTICULAR PURPOSE.

Exhibit E

LEXISNEXIS® RISK SOLUTIONS
REQUIRMENTS

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 lnc.'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 lnc.'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 lnteragency 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 lnc.'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 residents purpose limited to, obtaining the consent of Vermont residents prior to obtaining any information on Vermont through these Credit Technologies Inc. Services. In addition, Customer certifies it has a permissible 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 reason for 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 lnc.'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 lnc.'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 lnc.'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 in any 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 lnc.'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 lnc.'s obligations under its contracts with its data providers and Credit Technologies lnc.'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 lnc.'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 lnc.'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 CreditTechnologies 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: https://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. § 248oe (1999) § 248oe. 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 CF112 FAIRCREDITREPORTING CVRo6 •031•012, CF112.03 (1999) CF112.03 CONSUMER CONSENT

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 248oe 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. §§ 248oe 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. §§ 248oe 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 com ply 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.