

Exhibit A

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

All users subject to the Federal Trade Commission's jurisdiction must comply with all applicable regulations, including regulations promulgated after this notice was prescribed in 2004. Information about applicable regulations currently in effect can be found at the Commission's Web site, www.ftc.gov/credit. Persons not subject to the Commission's jurisdiction should consult with their regulators to find any relevant regulations.

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 Federal Trade Commission's Website at www.ftc.gov/credit. 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 Commission's Web site. **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 (CTI), you have additional obligations and will receive a separate notice from the CTI 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).2
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CTI

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 CTI (including a toll-free telephone number, if it is a nationwide CTI) that provided the report.
- A statement that the CTI 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 CTI if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CTI the accuracy or completeness of any information provided by the CTI.

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 CTI, 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..4

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 identity 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 CTIs, 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 Federal Trade Commission and the banking and credit union regulators. The Federal Trade Commission's regulations will be available at www.ftc.gov/credit.

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 Federal Trade Commission, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Federal Trade Commission's regulations may be found at www.ftc.gov/credit.

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 to be jointly prescribed by the Federal Trade Commission and the Federal Reserve Board. 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 information from a CTI 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 CTI 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 CTI.) A Section 615(a) adverse action notice should be sent after the adverse action is taken. An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2) The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CTI that conducts the investigation.)
- The user must certify to the CTI 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 as 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(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CTI a list of consumers who meet certain preestablished 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 to 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 CTI 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 CTI that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system. In addition, once the Federal Trade Commission by rule has established the format, type size, and manner of the disclosure required by Section 615(d), users must be in compliance with the rule. The FTC's regulations will be at www.ftc.gov/credit.

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 CTI.
- Identify to the source CTI 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 identity 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(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CTI for reinvestigation. When any CTI 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(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619. **The FTC's Web site, www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA. Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:**

Section 602 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 605A 15 U.S.C. 1681cA, Section 605B 15 U.S.C. 1681cB, Section 606 15 U.S.C. 1681d, Section 607 15 U.S.C. 1681e, Section 608 15 U.S.C. 1681f, Section 609 15 U.S.C. 1681g, Section 610 15 U.S.C. 1681h, Section 611 15 U.S.C. 1681i, Section 612 15 U.S.C. 1681j, Section 613 15 U.S.C. 1681k, Section 614 15 U.S.C. 1681l, Section 615 15 U.S.C. 1681m, Section 616 15 U.S.C. 1681n, Section 617 15 U.S.C. 1681o, Section 618 15 U.S.C. 1681p, Section 619 15 U.S.C. 1681q, Section 620 15 U.S.C. 1681r, Section 621 15 U.S.C. 1681s, Section 622 15 U.S.C. 1681s-1, Section 623 15 U.S.C. 1681s-2, Section 624 15 U.S.C. 1681t, Section 625 15 U.S.C. 1681u, Section 626 15 U.S.C. 1681v, Section 627 15 U.S.C. 1681w, Section 628 15 U.S.C. 1681x, Section 629 15 U.S.C. 1681y

Exhibit B

Equifax Requirements

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: (y) pursuant to FCRA Section 608 or (z) 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 must be reviewed for verification: the signature page; the address page; the terms of the lease page; landlord name and landlord contact information; (d) a copy of the principal's driver's license is required to verify the principal's identity; (e) 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 (f) 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. Reasonable measures include (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; and (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 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 ACROPAC OR ANY 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 EMPLOYMENT PURPOSES UNLESS CUSTOMER HAS A SUBSCRIPTION TO 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 2480e and applicable Vermont Rules. Customer further certifies that the attached copy of Section 2480e (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 Requirements

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 compromised. 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 Access Security Requirements

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

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

1. Implement Strong Access Control Measures

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

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

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

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

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

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

1.7 Develop strong passwords that are:

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

1.8 Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:

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

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

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

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

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

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

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

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

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

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

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

2. Maintain a Vulnerability Management Program

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

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

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

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

3. Protect Data

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

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

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

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

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

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

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

- 3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.
- 3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
- 3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

- 4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.
- 4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.
- 4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify Credit Technologies, Inc within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*
- 4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.
- 4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

5. Build and Maintain a Secure Network

- 5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.
- 5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
- 5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.
- 5.7 When using service providers (e.g. software providers) to access Experian systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

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

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

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

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

7. Mobile and Cloud Technology

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

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

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

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

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

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

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

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
 - oISO 27001
 - oPCI DSS
 - oEI3PA
 - oSSAE 16 – SOC 2 or SOC3
 - oFISMA
 - oCAI / CCM assessment

8. General

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

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Company individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Experian information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Experian information systems; this applies to both in-house or outsourced software development) based on the following requirements:

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

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example:

Internet Delivery Security Requirements

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

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. An officer of the Company agrees to notify Credit Technologies, Inc. in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Credit Technologies, Inc. immediately.
2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.

3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

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

Certify that the client shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Reseller must use the complete entire wording stated above or language substantially similar within the contract with the end user.

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

Acknowledge that many services containing Experian information also contain information from the Death Master File as issued by the Social Security Administration ("DMF"); certify pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102 that, consistent with its applicable FCRA or GLB use of Experian information, the client's use of deceased flags or other indicia within the Experian information is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules

regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1); and certify that the client will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian information.

Certify that the client shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Reseller must use the complete entire wording stated above or language substantially similar within the contract with the end user.

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential Encryption	Very sensitive information. Disclosure could adversely impact your company. Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven digit Experian account number. The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian.
Experian Independent Third Party Assessment Program	EI3PA SM requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA SM also establishes quarterly scans of networks for vulnerabilities.

ISO 27001 /27002

IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard)
The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.

Computer Virus

A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.

Confidential Encryption

Very sensitive information. Disclosure could adversely impact your company. Encryption is the process of obscuring information to make it unreadable without special knowledge.

Firewall

In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

Information Lifecycle

(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.

IP Address

A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone

Exhibit D

Trans Union Requirements

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

1. Customer certifies that Customer shall use the consumer reports: (a) solely for the Subscriber’s certified use(s); and (b) solely for Customer’s exclusive one-time use. Customer shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with Customer’s own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by Customer only to Customer’s designated and authorized employees having a need to know and only to the extent necessary to enable Customer to use the Consumer Reports in accordance with this Agreement. Customer shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.
2. Customer will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.
3. Customer shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that Customer may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its Customer for scores obtained from TransUnion, or as explicitly otherwise authorized in advance and in writing by TransUnion 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 election, 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),

Exhibit E Vermont Statute

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

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

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

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

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

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

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

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

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

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental benefit in a manner other than in writing, then the person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request. The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

(b) Consumer consent required pursuant to 9 V.S.A. §§ 2480e and 2480g shall be deemed to have been obtained in writing if, after a clear and adequate written disclosure of the circumstances under which a credit report or credit reports may be obtained and the purposes for which the credit report or credit reports may be obtained, the consumer indicates his or her consent by providing his or her signature.

(c) The fact that a clear and adequate written consent form is signed by the consumer after the consumer's credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent.

Exhibit F

California End User

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

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

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

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

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

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

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

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

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

Exhibit G

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 of such 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.