Appendix B: Notice to Users of Consumer Reports: Obligations of Users under the FCRA

1.0 INTRODUCTION

1.1 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.

1.2 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.

1.3 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**.

1.3.1 Persons not subject to the Commission's jurisdiction should consult with their regulators to find any relevant regulations.

1.3.2 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.**

1.4 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.

1.4.1 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.

2.0 OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

2.1 Users Must Have a Permissible Purpose

2.1.1 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)

***Appendix B Continued*:**

- 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. 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)

2.1.2 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.

2.2 Users Must Provide Certifications

2.2.1 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.

2.3 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.

2.3.1 Adverse Actions Based on Information Obtained From a CRA

2.3.1.1 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.

Appendix B Continued

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.

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

2.3.2.2 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.

2.3.3 Adverse Actions Based on Information Obtained From Affiliates

2.3.3.1 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 2.3.1 above.

2.3.4 Military Alerts are in Files

2.3.4.1 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.

Appendix B Continued:

2.3.4.2 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

2.3.4.3 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.

2.3.5 Users Have Obligations When Notified of an Address Discrepancy

2.3.5.1 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.

2.3.5.2 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**.

2.3.6 Users Have Obligations When Disposing of Records

2.3.6.1 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**.

3.0 CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

3.1 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.

3.2 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").

4.0 OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

4.1 Employment Other Than in the Trucking Industry

4.1.1 If 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.

Appendix B Continued:

- 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.
- 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

4.2 Employment in the Trucking Industry

4.2.1 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.

4.2.2 The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

5.0 OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

5.1 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.)

Appendix B Continued:

- 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.

6.0 SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

6.1 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.

6.2 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.

7.0 OBLIGATIONS OF USERS OF MEDICAL INFORMATION

7.1 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).

7.2 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.

7.3 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.

7.4 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).

8.0 OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

8.1 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)).

8.2 This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must:

Appendix B Continued:

8.2.1 (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

8.2.2 (2) Maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer.

8.2.3 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.

8.2.4 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.**

9.0 OBLIGATIONS OF RESELLERS

9.1 Disclosure and Certification Requirements

9.1.1 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 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

Appendix B Continued:

9.2 Reinvestigations by Resellers

9.2.1 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 CRA for reinvestigation.

9.2.2 When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

9.3 Fraud Alerts and Resellers

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

10.0. LIABILITY FOR VIOLATIONS OF THE FCRA

10.1 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).

10.2 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.

10.3 Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

Section 602 Section 603 Section 604 Section 605 Section 605A Section 605B Section 606 Section 607 Section 608 Section 609 Section 610 Section 611 Section 612 Section 613 Section 614 Section 615 Section 616 Section 617 Section 618 Section 619 Section 620 Section 621 Section 622 Section 623 Section 624 Section 625 Section 626 Section 627 Section 628 Section 629 15 U.S.C. 1681 15 U.S.C. 1681a 15 U.S.C. 1681b 15 U.S.C. 1681c 15 U.S.C. 1681cA 15 U.S.C. 1681cB 15 U.S.C. 1681d 15 U.S.C. 1681e 15 U.S.C. 1681f 15 U.S.C. 1681g 15 U.S.C. 1681h 15 U.S.C. 1681i 15 U.S.C. 1681j 15 U.S.C. 1681k 15 U.S.C. 1681/ 15 U.S.C. 1681m 15 U.S.C. 1681n 15 U.S.C. 1681o 15 U.S.C. 1681p 15 U.S.C. 1681q 15 U.S.C. 1681r 15 U.S.C. 1681s 15 U.S.C. 1681s-1 15 U.S.C. 1681s-2 15 U.S.C. 1681t 15 U.S.C. 1681u 15 U.S.C. 1681v 15 U.S.C. 1681w 15 U.S.C. 1681x 15 U.S.C. 1681y

Appendix C: Businesses That Cannot Be Provided Information

- Adult entertainment service of any kind
- Business that operates out of an apartment or unrestricted location within a residence (unless approved by repository)
- Attorneys or Law Offices of any type
- Bail bondsman
- Check cashing
- Credit counseling
- Credit repair clinic
- Dating service
- Financial counseling
- Genealogical or heir research firm
- Massage services
- Company that locates missing children
- Pawn shop
- Private detectives, detective agencies or investigative companies
- Individual seeking information for their private use
- Company that handles third party repossession
- Company or individual involved in spiritual counseling
- Subscriptions (magazines, book clubs, record clubs, etc.)
- Tattoo service
- Insurance Claims
- Internet Locator Services
- Asset Location Services
- Future Services (i.e., health clubs, timeshare, continuity clubs, etc.)
- News Agencies or journalists
- Law Enforcement (except for employment screening)
- Any company or individual who is known to have been involved in credit fraud or other
- unethical business practices
- Companies listed on repository alert report notifications

Appendix D: Equifax Requirements

Customer, in order to receive consumer credit information from Equifax Information Services, LLC, through CPI 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 CPI 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.

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

2.0 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.

2.1 Subscriber, 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 FCPI Section 608 or (z) for an investigation on a matter related to public safety.

2.2 Customer further certifies that it will, with each Limited ID or Limited DTEC inquiry, include the Exception Code required by Equifax that identifies the use for which Customer is ordering the information, and that because Limited ID and Limited DTEC reports are not consumer reports;

Appendix D: Equifax Requirements continued

2.2.1 Customer will not order or use Limited ID or Limited DTEC reports, in whole or in part, to determine eligibility for credit, insurance, or for any other permissible purpose, as defined by the FCPI, for which a consumer reporting agency is permitted to furnish a consumer report.

2.3 Equifax may periodically conduct audits of Customer regarding its compliance with the FCPI and other certifications in this Agreement. Audits will be conducted by mail whenever possible and will require Subscribers to provide documentation as to permissible use of particular consumer, Limited ID, or Limited DTEC reports.

2.3.1 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.

2.3.2 If Equifax terminates this Agreement due to the conditions in the preceding sentence, Subscriber

(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.

3.0 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

4.0 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 CPI 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 CPI 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.

Appendix D: Equifax Requirements continued

5.0 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.

5.1 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.

5.2 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.

5.3 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.

5.4 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.

6.0 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 CPI 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 CPI 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.

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

7.0 Customer will be charged for Equifax consumer credit information by CPI, which is responsible for paying Equifax for such information; however, should the underlying relationship between CPI 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.

Appendix D: Equifax Requirements continued

8.0 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.

8.1 A Subscriber 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.

9.0 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 duly and fully perform its obligations under this Agreement, the denial of service to Customer by Equifax, the misuse or improper access to Equifax consumer credit information by Customer or the failure of Customer to comply with applicable laws or regulations.

9.1 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.

Appendix D: Equifax Requirements continued

10.0 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 SUBSCRIBER.

Appendix D-2: Additional Equifax Information Services

This Appendix D-2 supplements the service agreement ("Agreement") under which Customer receives, as part of its service from CPI, consumer credit report information available from Equifax Information Services LLC ("Equifax").

This Appendix contains additional information services available from Equifax, described below, that may be provided to Customer subject to the terms and conditions of the Agreement, and additional terms and conditions that apply to such additional information services.

Customer's authorized representative must place his or her initials by each service listed below that Customer desires to receive. Customer agrees to abide by the additional terms and conditions that apply to the service(s) so selected.

_____BEACON

_____Pinnacle K

_____SafeScan

_____PERSONA

1.0 BEACON[SM] is a consumer report credit scoring service based on a model developed by Fair, Isaac and Equifax that ranks consumers in the Equifax consumer credit database relative to other consumers in the database with respect to the likelihood of those consumers paying their accounts as agreed ("Score").

2.0 Pinnacle[SM] is a credit scoring algorithm developed by Fair, Isaac and Equifax that evaluates the likelihood that consumers will pay their existing and future credit obligations, as agreed, based on the computerized consumer credit information in the Equifax consumer reporting database.

2.1 (a) Disclosure of Scores: Customer will hold all information received from Equifax in connection with any Score received from Equifax under this Agreement in strict confidence and will not disclose that information to the consumer or to others except in accord with the following sentence or as required or permitted by law.

- Customer may provide the principal factors contributing to the Score to the subject of the report when those principal factors are the basis of Customer's adverse action against the subject consumer.
- Customer must describe the principal factors in a manner which complies with Regulation B of the ECOA.

2.2 (b) ECOA Statements: Equifax reasonably believes that, subject to validation by Customer on its own records,

(1) the scoring algorithms used in the computation of the Score are empirically derived from consumer credit information from Equifax's consumer credit reporting database, and are demonstrably and statistically sound methods of rank ordering candidate records from the Equifax consumer credit database for the

Appendix D-2: Additional Equifax Information Services continued

purposes for which the Score was designed particularly, and it is intended to be an "empirically derived, demonstrably and statistically sound credit scoring system" as defined in Regulation B, with the understanding that the term "empirically derived, demonstrably and statistically sound," is defined only in a generalmanner by Regulation B, and has not been the subject of any significant interpretation; and

(2) the scoring algorithms comprising the Score, except as permitted, do not use a "prohibited basis," as such phrase is defined in Regulation B. Customer must validate the Score on its own records. Customer will be responsible for meeting its requirements under the ECOA and Regulation B.

2.3 (c) Release: Equifax does not guarantee the predictive value of the Score with respect to any individual, and does not intend to characterize any individual as to credit capability.

- Neither Equifax nor its directors, officers, employees, agents, subsidiary and affiliated companies, or any third-party contractors, licensors or suppliers of Equifax will be liable to Customer for any damages, losses, costs or expenses incurred by Customer resulting from any failure of a Score to accurately predict the credit worthiness of Customer's applicants or customers. In the event the Score is not correctly applied by Equifax to any credit file, Equifax's sole responsibility will be to reprocess the credit file through the Score at no additional charge.

2.4 (d) Audit of Models: Customer may audit a sample of the Scores and principal factors and compare them to the anonymous underlying credit reports in accordance with Equifax's audit procedures.

2.4.1 If the Scores and principal reasons are not substantiated by the credit files provided for the audit, Equifax will review programming of the model and make corrections as necessary until the Scores and principal reasons are substantiated by the audit sample credit reports.

2.4.2 After that review and approval, Customer will be deemed to have accepted the resulting Score and principal factors delivered. It is Customer's sole responsibility to validate all scoring models on its own records and performance

2.5 (e) Confidentiality: Customer will hold all Scores received from Equifax under this Agreement in strict confidence and will not disclose any Score to the consumer or to others except as required or permitted by law.

2.5.1 Customer may provide the principal factors contributing to the Score to the subject of the report when those principal factors are the basis of Customer's adverse action against the subject consumer.

2.5.2 Customer must describe the principal factors in a manner which complies with Regulation B of the ECOA.

Appendix D-2: Additional Equifax Information Services continued

2.5.3 Further, Customer acknowledges that the Score and factors are proprietary and that, Customer will not provide the Score to any other party without Equifax's and Fair, Isaac's prior written consent except for:

- (a)disclosure to the subject consumer if Customer has taken adverse action against such consumer based in whole or in part on the consumer report with which the Score was delivered or
- (b) as required by law,

2.6 (f) Limited Liability: The combined liability of Equifax and Fair, Isaac arising from any particular Score provided by Equifax and Fair, Isaac shall be limited to the aggregate amount of money received by Equifax from Customer with respect to that particular Score during the preceding twelve (12) months prior to the date of the event that gave rise to the cause of action.

2.7 (g) Adverse Action: Customer shall not use a Score as the basis for an "Adverse Action" as defined by the Equal Credit Opportunity Action or Regulation B, unless score factor codes have been delivered to Customer along with the Score.

3.0 SAFESCAN®

3.1 SAFESCAN is an on-line warning system containing information that can be used to detect possible fraudulent applications for credit. Some of the information in the SAFESCAN database is provided by credit grantors. SAFESCAN is a registered trademark of Equifax.

3.2 Permitted Use. SAFESCAN is not based on information in Equifax's consumer reporting database and is not intended to be used as a consumer report.

3.2.1 Customer will not use a SAFESCAN alert or warning message in its decision-making process for denying credit or any other FCRA permissible purpose, but will use the message as an indication that the consumer's application information should be independently verified prior to a credit or other decision.

3.2.2 Customer understands that the information supplied by SAFESCAN may or may not apply to the consumer about whom Customer has inquired.

4.0 PERSONA® and PERSONA PLUS®

4.1 PERSONA® and PERSONA PLUS® - are consumer reports, from the Equifax consumer credit database, consisting of limited identification information, credit file inquiries, public record information, credit account trade lines, and employment information.

4.2 FCPI Certification: Customer will notify Equifax whenever a consumer report will be used for employment purposes.

4.2.1 Customer certifies that, before ordering each consumer report to be used in connection with employment purposes, it will clearly and conspicuously disclose to the subject consumer, in a written document consisting solely of the disclosure, that Customer may obtain a consumer report for employment purposes, and will also obtain the consumer's written authorization to obtain or procure a consumer report relating to that consumer.

4.2.2 Customer further certifies that it will not take adverse action against the consumer based in whole or in part upon the consumer report without first providing to the consumer to whom the consumer report relates a copy of the consumer report and a written description of the consumer's rights as prescribed by the Federal Trade Commission ("FTC") under Section 609(c)(3) of the FCRA, and will also not use any information from the consumer report in violation of any applicable federal or state equal employment opportunity law or regulation.

4.2.3 Customer acknowledges that it has received from Equifax a copy of the written disclosure form pre-scribed by the FTC.

Appendix E-1: 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 CPI 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.

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

2.0 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.

2.1.1 Customer authorizes CPI to provide to Experian, upon Experian's request, all materials and information relating to its investigations of Customer.

2.1.2 Customer further agrees that it will respond within the requested time frame indicated for information requested by Experian regarding Experian consumer credit information.

2.1.3 Customer understands that Experian may require CPI 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 CPI prior to any such discontinuance.

3.0 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.

Appendix E-1: Experian Requirements continued

4.0 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:

4.1.1 (a) Customer will notify CPI 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 CPI or Experian that results from Customer's breach of Experian consumer credit information.

4.1.2 (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.

4.1.3 (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.

4.1.4 (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.

5.0 Customer understands that if a change of control or ownership should occur, the new owner of the Customer business must be re-credentialed as a permissible and authorized Customer of Experian products and services. A third party physical inspection at the new address will be required if Customer changes location.

6.0 If Customer is an authorized residential customer the following additional requirements and documentation must be supplied:

6.1.1 (a) Experian must be notified for tracking and monitoring purposes;

6.1.2 (b) Customer must maintain a separate business phone line listed in the name of the business;

6.1.3 (c) A separate subscriber code for Customer must be maintained for compliance monitoring; and

6.1.4 (d) An annual physical inspection of the office is required by Experian, for which a reasonable fee may be required.

Appendix E-1: Experian Requirements continued

7.0 Customer agrees to hold harmless Experian and its agents from and against any and all liabilities, damages, losses, claims, costs and expenses, including reasonable attorney's fees, which may be asserted against or incurred by Experian, arising out of or resulting from the use, disclosure, sale or transfer of the consumer credit information by Customer, or Customer's breach of this Agreement.

7.1.1 Customer further understands and agrees that the accuracy of any consumer credit information is not guaranteed by Experian and releases Experian and its agents 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 Experian.

8.0 Experian will not, for the fee charged for credit information, be an insurer or guarantor of the accuracy or reliability of the information.

8.1.1 EXPERIAN DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE INFORMATION AND SHALL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY EXPERIAN'S ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE INFORMATION.

Appendix E-2: Experian FICO Notice

Terms of End-User Contracts: All contracts between Reseller and Reseller Customers for the resale of the Experian/Fair, Isaac Advanced Risk Score(s) and reason codes generated by the Experian/Fair, Isaac Advanced Model shall contain the following provisions, each of which is material.

1.0 A description of the applicable product(s) and/or service(s);

2.0 A provision in which Reseller Customer releases Fair, Isaac and/or Experian as well as their respective officers, directors, employees, agents, sister or affiliated companies, or any third party contractors or suppliers of Fair, Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by Reseller Customer resulting from any failure of the Experian/Fair, Isaac Advanced Risk Score(s) to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily;

3.0 A provision extending certain of Fair, Isaac's and Experian's warranties and indemnities in Sections 3 and 6 of this Addendum to the Reseller Customer (subject to the applicable terms and conditions as specified in Sections 3 and 6);

4.0 A provision limiting the combined liability of Experian and Fair, Isaac to the Reseller Customer to the fees received from the Reseller Customer for use of the Experian/Fair, Isaac Advanced Risk Score(s) in the preceding twelve (12) months;

5.0 A provision certifying that the Reseller Customer has a permissible purpose for obtaining the Experian/Fair, Isaac Advanced Risk Score(s);

6.0 A provision whereby Reseller Customer certifies that any use of the Experian/Fair, Isaac Advanced Risk Model for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, or the Fair Credit Reporting Act.

7.0 A statement that the Experian/Fair, Isaac Advanced Risk Score(s) shall not be used for adverse action as defined by the ECOA or Regulation B, unless adverse action reason codes have been delivered to the Reseller Customer along with the Experian/Fair, Isaac Advanced Risk Score(s);

8.0 A provision certifying that the Reseller Customer acknowledges that the Experian/Fair, Isaac Advanced Risk Score(s) and its associated intellectual property rights in its output are the property of Fair, Isaac and that Reseller Customer will not provide the Experian/Fair, Isaac Advanced Risk Score(s) to any other party without Fair, Isaac's and Experian's prior written consent except

(1) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes or

(2) as clearly required by law

9.0 A provision certifying that the Reseller Customer will not publicly disseminate any results of the validations or other reports derived from the Experian/Fair, Isaac Advanced Risk Score or the Experian/Fair, Isaac Advanced Risk Score(s) without Fair, Isaac's and Experian's express written permission; and,

Appendix E-2: Experian FICO Notice continued

10.0 An agreement that Reseller Customer will, before delivering or directing Experian/Fair, Isaac to deliver Experian/Fair, Isaac Advanced Risk Score(s) to any third party (including any Third Party Processor), enter into a contract with such third party that

(1) limits the use of the Experian/Fair, Isaac Advanced Risk Score(s) by the third party only to the use permitted to the Reseller Customer and

(2) identifies Experian and Fair, Isaac as the express third party beneficiary of such contract.

Appendix F: Trans Union Requirements

Customer, in order to receive consumer credit information from Trans Union, LLC, through CPI, 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 CPI 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.

1.0 Customer hereby agrees to comply with all current and future policies and procedures instituted by CRA and required by Trans Union.

1.1.1 CPI will give Customer as much notice as possible prior to the effective date of any such new policy required in the future, but does not guarantee that reasonable notice will be possible.

1.1.2 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.

2.0 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.

3.0 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.

3.1.1 Customer authorizes CPI 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.

3.1.2 Customer understands that Trans Union may require CPI to suspend or terminate access to Trans Union's information in the event Customer does not cooperate with any such an investigation.

3.1.3 Customer shall remain responsible for the payment for any services provided to Customer prior to any such discontinuance.

Appendix F: Trans Union Requirements continued

4.0 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.

4.1.1 If approved by Trans Union and authorized by the consumer, Customer may deliver the consumer credit information to a third party, secondary, or joint user with which Customer has an ongoing business relationship for the permissible use of such information.

4.1.2 Customer understands that Trans Union may charge a fee for the subsequent delivery to secondary users.

5.0 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

5.1.1 THE WARRANTY SET FORTH IN THE PREVIOUS SENTENCE IS THE SOLE WARRANTY MADE BY TRANS UNION CONCERNING THE CONSUMER REPORTS, INCLUDING, BUT NOT LIMITED TO THE TU SCORES. TRANS UNION MAKES NO OTHER REPRESENTATIONS OR WARRANTIES INCLUDING, BUT NOT LIMITED TO, ANY REPRESENTATIONS OR WARRANTIES REGARDING THE ACCURACY, COMPLETENESS, OR BOTH, OF ANY AND ALL OF THE AFOREMENTIONED PRODUCTS AND SERVICES THAT MAY BE PROVIDED TO CRA. THE WARRANTY SET FORTH IN THE FIRST SENTENCE OF THIS PARAGRAPH IS IN LIEU OF ALL OTHER WARRANTIES, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, BUT NOT LIMITED TO, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

APPENDIX G TRANS UNION REQUIREMENTS

REGARDING CREDIT SCORING SERVICES

CLASSIC$_{sm}$ CREDIT RISK SCORE SERVICES

(Required Terms for Addendum to Subscriber Agreement for Consumer Reports between Reseller and its Customer)

1.0 Based on an agreement with Trans Union LLC ("Trans Union") and Fair Isaac Corporation ("Fair Isaac") ("Reseller Agreement"), CPI has access to a unique and proprietary statistical credit scoring service jointly offered by Trans Union and Fair Isaac which evaluates certain information in the credit reports of individual consumers from Trans Union's data base ("Classic") and provides a score which rank orders consumers with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring (the "Classic Score").

2.0 Customer, from time to time, may desire to obtain Classic Scores from Trans Union via an on-line mode in connection with consumer credit reports.

3.0 Customer has previously represented and now, again represents that it is a _____ and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").

4.0 Customer certifies that it will request Classic Scores pursuant to procedures prescribed by CPI from time to time only for the permissible purpose certified above, and will use the Classic Scores obtained for no other purpose.

5.0 Customer will maintain copies of all written authorizations for a minimum of three (3) years from the date of inquiry

6.0 Customer agrees that it shall use each Classic Score only for a one-time use and only in accordance with its permissible purpose under the FCRA.

7.0 With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, CPI may, upon its election, discontinue serving the Customer and cancel this Agreement, in whole or in part (e.g., the services provided under this Addendum only) immediately.

8.0 Customer recognizes that factors other than the Classic Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors.

9.0 Trans Union and Fair Isaac shall be deemed third party beneficiaries under this Addendum.

10.0 Up to five score reason codes, or if applicable, exclusion reasons, are provided to Customer with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg. B").

APPENDIX G TRANS UNION Requirements Continued

Regarding credit scoring services; CLASSICsm CREDIT RISK SCORE SERVICES

10.1 However, the Classic Score itself is proprietary to Fair Isaac, may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party, except:

(1) To credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or

(2) As clearly required by law. Customer will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and Trans Union's prior written consent

11.0 In the event Customer intends to provide Classic Scores to any agent, Customer may do so provided, however, that Customer first enters into a written agreement with such agent that is consistent with Customer's obligations under this Agreement.

11.1 Moreover, such agreement between Customer and such agent shall contain the following obligations and acknowledgments of the agent:

(1) Such agent shall utilize the Classic Scores for the sole benefit of Customer and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit;

(2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party without Trans Union and Fair Isaac's prior written consent except

(a) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or

(b) as clearly required by law;

(3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration;

(4) Such agent shall not resell the Classic Scores; and

(5) Such agent shall not use the Classic Scores to create Classic Scores to create or maintain a database for itself or otherwise

12.0 Customer acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information will result in an inquiry being added to the consumer's credit file.

13.0 Customer shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject.

APPENDIX G TRANS UNION Requirements Continued

14.0 The information including, without limitation, the consumer credit data, used in providing Classic Scores under this Agreement were obtained from sources considered to be reliable.

14.1 However, due to the possibilities of errors inherent in the procurement and compilation of data involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed.

14.2 Moreover, in no event shall Trans Union, Fair Isaac, nor their officers, employees, affiliated companies or bureaus, independent contractors or agents be liable to Customer for any claim, injury or damage suffered directly or indirectly by Customer as a result of the inaccuracy or incompleteness of such information used in providing Classic Scores under this Agreement and/or as a result of Customer's use of Classic Scores and/or any other information or serviced provided under this Agreement.

15.0 Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to Trans Union and used in the computation of the Classic Score ("Models") are empirically derived from Trans Union's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and Regulation B promulgated there under

15.1 Classic provides a statistical evaluation of certain information in Trans Union's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring relative to other individuals in Trans Union's database. The score may appear on a credit report for convenience only, but is not a part of the credit report nor does it add to the information in the report on which it is based.

15.2 THE WARRANTIES SET FORTH IN SECTION 15.1 ARE THE SOLE WARRANTIES MADE UNDER THIS ADDENDUM CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANS UNION MAKE ANY OTHER REPRESENTATIONS OR WARRANTIES CONCERNING THE PRODUCTS AND SERVICES TO BE PROVIDED UNDER THIS AGREEMENT OTHER THAN AS SET FORTH IN THIS ADDENDUM.

15.2.1 THE WARRANTIES AND REMEDIES SET FORTH IN SECTION 15.1 ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

APPENDIX G TRANS UNION Requirements Continued

16.0 IN NO EVENT SHALL ANY PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY THE OTHER PARTIES AND ARISING OUT OF THE PERFORMANCE OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF GOOD WILL AND LOST PROFITS OR REVENUE, WHETHER OR NOT SUCH LOSS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

17.0 THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO CUSTOMER, IN NO EVENT SHALL THE AFORESTATED LIMITATIONS OF LIABILITY, SET FORTH ABOVE IN SECTION 16, APPLY TO DAMAGES INCURRED BY TRANS UNION AND/OR FAIR ISAAC AS A RESULT OF:

(A) GOVERNMENTAL, REGULATORY OR JUDICIAL ACTION(S) PERTAINING TO VIOLATIONS OF THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM CUSTOMER'S BREACH, DIRECTLY OR THROUGH CUSTOMER'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT.

18.0 ADDITIONALLY, NEITHER TRANS UNION NOR FAIR ISAAC SHALL BE LIABLE FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL TRANS UNION'S AND FAIR ISAAC'S AGGREGATE TOTAL LIABILITY, IF ANY, UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY CUSTOMER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS ($10,000.00), WHICHEVER AMOUNT IS LESS.

19.0 This Addendum may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this Addendum by Customer; (2) in the event the agreement(s) related to Classic between Trans Union, Fair Isaac and CRA are terminated or expire; (3) in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation by any governmental entity.

APPENDIX H: State Compliance Matters

California Retail Seller

1.0 Provisions of the California Consumer Credit Reporting Agencies Act, as amended effective July 1, 1998, will impact the provision of consumer reports to Customer under the following circumstances:

(a) if Customer is a "retail seller" (defined in part by California law as "a person engaged in the business of selling goods or services to retail buyers") and is selling to a "retail buyer" (defined as "a person who buys goods or obtains services from a retail seller in a retail installment sale and not principally for the purpose of resale") and a consumer about whom Customer is inquiring is applying,

(b) in person, and

(c) For credit

2.0 Under the foregoing circumstances, Equifax, before delivering a consumer report to Customer, must match at least three (3) items of a consumer's identification within the file maintained by Equifax with the information provided to Equifax by Customer in connection with the in-person credit transaction. Compliance with this law further includes Customer's inspection of the photo identification of each consumer who applies for in-person credit, mailing extensions of credit to consumers responding to a mail solicitation at specified addresses, taking special actions regarding a consumer's presentment of a police report regarding fraud, and acknowledging consumer demands for reinvestigations within certain time frames

3.0 If Customer is a "retail seller," Customer certifies that it will instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person. If Customer is not currently, but subsequently becomes a "retail seller," Customer agrees to provide written notice to Equifax prior to ordering credit reports in connection with an in-person credit transaction, and agrees to comply with the requirements of the California law as outlined in this Section, and with the specific certifications set forth herein.

4.0 Customer certifies that, as a "retail seller," it will either:

(a) Acquire a new Customer number for use in processing consumer report inquiries that result from in-person credit applications covered by California law, with the understanding that all inquiries using this new Customer number will require that Customer supply at least three items of identifying information from the applicant; or

(b) Contact Customer's Equifax sales representative to ensure that Customer's existing number is properly coded for these transactions.

APPENDIX I Equifax Requirement

VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

1.0 Customer acknowledges that it subscribes to receive various information serviced from Equifax Credit Information Services, Inc. ("Equifax") in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts.

1.1. In connection with Customer's continued use of Equifax information services in relation to Vermont consumers, Customer hereby certifies as follows:

1.1.1 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 VFCRA, only after Customer has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules.

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

2.1 § 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

APPENDIX I Equifax Requirement continued

VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

3.0 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

3.1 (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.

3.1.1 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 is 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.

3.1.2 The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

3.2 (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.

3.3 (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.

APPENDIX J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data

Introduction

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information.

It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you.

Credit Plus Inc. (CPI) reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security. These requirements are applicable to all systems and devices used to access, transmit, process, or store credit reporting agency data:

1.0 Implement Strong Access Control Measures

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

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

1.3 If the third party or third party software or proprietary system or software, used to access CPI 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 CPI'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)alpha/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)

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

1.8 Passwords (e.g. user/account 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 algorithms 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.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

2.0 Maintain a Vulnerability Management Program

2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.

2.2 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, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3.0 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.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

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).

4.0 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 Safeguard 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 CPI 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 your 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 the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers.
- If the service provider is in the process of becoming compliant, it is Company's responsibility to ensure the service provider is engaged with Experian and an exception is granted in writing.
- Approved certifications in lieu of EI3PA can be found in the Glossary section.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

5.0 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 CPI systems, access to third party tools/services must require multi-factor authentication.

6.0 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 CPI 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

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

7.0 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:

7.7.1 Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations

7.7.2 Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:

- ISO 27001
- PCI DSS
- EI3PA
- SSAE 16 – SOC 2 or SOC3
- FISMA
- CAI / CCM assessment

8.0 General

8.1 CPI 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

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to CPI 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 CPI 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 CPI 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: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software 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

8.5 Reasonable access to audit trail reports of systems utilized to access CPI systems shall be made available to CPI upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to CPI must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to CPI within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to CPI of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at CPI: 800-258-3488. Email notification will be sent to CPI: compliance@creditplus.com

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to CPI services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of CPI networking and computing resources may be monitored and audited by CPI without further notice.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/authorized users, and for assuring that mechanisms to access CPI services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by CPI.

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

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

9.0 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 CPI provided services via Internet ("Internet Access").

9.1 General requirements:

9.1.1 The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with CPI on systems access related matters.

- The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to CPI provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

9.1.2 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 CPI product based upon the legitimate business needs of each employee.
- CPI shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.

9.1.3 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 CPI.

- 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).

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

- CPI's approval of requests for (Internet) access may be granted or withheld in its sole discretion.
- CPI 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.

9.1.4 An officer of the Company agrees to notify CPI 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

9.2 Roles and Responsibilities

9.2.1 Company agrees to identify an employee it has designated to act on its behalf as a primary interface with CPI 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 CPI on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users.
- 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 CPI's systems and information (via the Internet).
- Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to CPI immediately.

9.2.2 As a Client to CPI's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company

9.2.3 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 CPI 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).

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

- 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 CPI's Security Administration group on information and product access matters.

9.2.4 The Head Designate shall be responsible for notifying their corresponding CPI 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.

9.3 Designate

9.3.1 Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.

9.3.2 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.).

9.3.3 Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

9.3.4 Is responsible for ensuring that Company's Authorized Users are authorized to access CPI products and services.

9.3.5 Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.

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

9.3.7 Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to CPI.

9.3.8 Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.

9.3.9 Shall be available to interact with CPI when needed on any system or user related matters.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

10.0 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	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have 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.

Appendix J: Experian Access Security Requirements for Reseller End-Users, FCRA and GLB 5A Data Continued:

Term	Definition
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ 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.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report, just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Appendix K: Trans Union Score Disclosure

1.0 End User will request Scores only for End User's exclusive use.

1.1 End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining the Scores.

1.2 End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score.

2.0 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:

2.1 To those employees of End User with a need to know and in the course of their employment;

2.2 To those third party processing agents and other contractors of End User who have executed an agreement that limits the use of the Scores by the third party only to the use permitted to End User and contains the prohibitions set forth herein regarding model development, model calibration, reverse engineering and confidentiality;

2.3 When accompanied by the corresponding reason codes, to the consumer who is the subject of the Score;

2.4 To government regulatory agencies; or

2.5 As required by law.

Appendix L: Death Master File

1.0 INTRODUCTION

1.1 Certain data provided by Credit Plus, Inc. as part of its service offerings includes information obtained from the Death Master File (DMF) made available by the US Department of Commerce National Technical Information Service (NTIS) and subject to regulations found at 15 CFR Part 1110.

1.2 All Credit Plus, Inc. customers, including End Users, are required to comply with all applicable laws including, with respect to DMF data, 15 CFR Part 1110.

1.3 Recipients of DMF data that fail to comply with 15 CFR Part 1110 may be subject to, among other things, penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

2.0 Based on the requirements of NTIS and 15 CFR Part 1110, End User agrees to the following:

2.1 (a) **Certified Person** End User shall ensure that it meets the requirements of a Certified Person under 15 CFR Part 1110.2.

2.2 (b) **Security** End User shall have systems, facilities, and procedures in place to safeguard the information received from the DMF; experience in maintaining the confidentiality, security, and appropriate use of the accessed information, pursuant to requirements similar to the requirements of section 6103(p) (4) of the Internal Revenue Code of 1986; and agrees to satisfy the requirements of such section 6103(p) (4) as if such section applied to End User.

2.3 (c) **End User** shall not, with respect to information derived from the DMF: Disclose such deceased

I. Individual's DMF to any person other than a person who meets the requirements of a.i.(1) and (2) above;

II. Disclose such deceased individual's DMF to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty;

III. Disclose such deceased individual's DMF to any person who further discloses the information to any person other than a person who meets the requirements of a.i.(1) and (2) above;

IV. Use any such deceased individual's DMF for any purpose other than a legitimate fraud prevention purpose or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty.

2.4 (d) **Penalties** End User acknowledges that failure to comply with the provisions in a) and b) above may subject End User to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year. In all other respects, the Agreement shall remain in full force and effect, except as expressly modified hereby.

Appendix L: Death Master File continued

2.5 (e) **Indemnification and Hold Harmless** End User shall indemnify and hold harmless CPI, TransUnion, Equifax Information Services, Experian Information Solutions and the U.S. Government/NTIS from all claims, demands, damages, expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with CPI, CPI's employees, contractors, subcontractors, or End Users' use of the DMF.

2.5.1 This provision shall survive termination of the Agreement and will include any and all claims or liabilities arising from intellectual property rights.

2.6 (f) **Liability**

(I) Neither CPI, nor the U.S. Government/NTIS:

(a) make any warranty, express or implied, with respect to information provided under this Section of the Policy, including, but not limited to, implied warranties of merchantability and fitness for any particular use;

(b) assume any liability for any direct, indirect or consequential damages flowing from any use of any part of the DMF, including infringement of third party intellectual property rights; and

(c) Assume any liability for any errors or omissions in the DMF. The DMF does have inaccuracies and NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, does not guarantee the accuracy of the DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the DMF.

(II) If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the DMF), the individual should be told to contact to their local Social Security office (with proof) to have the error corrected. The local Social Security office will:

(a) Make the correction to the main NUMIDENT file at SSA and give the individual a verification document of SSA's current records to use to show any company, recipient/purchaser of the DMF that has the error; OR,

(b) Find that SSA already has the correct information on the main NUMIDENT file and DMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company subscriber/ purchaser of the DMF that had the error.

Appendix M: Information Security Requirements

1.0 Certify that the client shall implement and maintain a comprehensive Information Security Program written in one or more readily accessible parts that contains administrative, technical, and physical safeguards appropriate to:

- The client's size and complexity,
- The nature and scope of its activities
- Sensitivity of the information provided to the client by End User

2.0 Such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to:

2.1 Insure the security and confidentiality of the information provided by End User

2.2 Protect against any anticipated threats or hazards to the security or integrity of such information

2.3 Protect against unauthorized access or use of such information that could result in substantial harm or inconvenience to any consumer.