



ADDENDUM A

1. This is Addendum A to the MAF Background Screening Application for Services and is made a part of said Agreement. By accepting and signing below, Customer hereby agrees to comply with all terms and conditions of the MAF Background Screening Application for Services, Addendum A and all Exhibits and Appendices which are explicitly made a part hereof

2. MAF Background Screening may from time to time diminish or increase the charges to Customer upon thirty days' written notice mailed or delivered to Customer at its business address and in such event Customer agrees to pay to revised charges unless Customer shall terminate this Addendum as hereinafter provided.

3. Customer hereby agrees, represents and warrants that it intends to use services for the purposes of tenant screening and/or employment background screening and in using the services of MAF Background Screening, Customer will in all respects comply with the provisions of 15 U.S.C. §1681 *et seq.* ("FCRA") and that services will be requested only for the Customer's exclusive use.

4. Customer certifies that it will request consumer reports pursuant to procedures prescribed by MAF Background Screening from time to time and only for the permissible purpose certified above, and will use the reports obtained for no other purpose. Customer shall use each consumer report only for a one-time use and shall hold the report in strict confidence, and not to disclose it to any third parties; provided, however that Customer may, where allowed or required by law, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, for scores obtained from Trans Union, Equifax Information Services, or Experian Information Solutions, Customer shall not disclose to consumers or any third party, any or all such scores provided under this Addendum, except as required by law. Customer agrees that consumer credit reports on employees will not be requested. The employment consumer report is to be accessed when pulling reports on employees. Customer will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry and provide MAF Background Screening copies of such upon request. Customer further agrees, as requested, promptly to furnish by telephone or in writing to MAF Background Screening all required information covering transactions by the Customer and its consumers, and to indemnify MAF Background Screening, Trans Union, Equifax Information Services, Experian Information Solutions, and each of the other Customers and the officers and employees of each, jointly and severally, from any loss, damage, attorney's fees and costs arising from any claim or suit based on alleged violation of any provision of this Addendum.

5. This Addendum shall continue in force without any fixed date of termination, subject to cancellation by either party upon thirty (30) days prior written notice mailed or delivered to the office of the other party; further subject to the right of MAF Background Screening at any time and without prior notice, to terminate this Addendum in event of any federal or state law or decision which affects the economic operation of MAF Background Screening or any violation by Customer of any provision of this Addendum or the FCRA, and further subject to the right of Customer at any time and without prior written notice, to terminate this Addendum in event of increase in charges to the Customer, as provided herein.

6. No information furnished to Customer is guaranteed nor is MAF Background Screening in any way responsible for such information. MAF Background Screening shall not be responsible or liable for any loss caused by neglect or act of any of its servants, agents, attorneys, clerks or employees in procuring, collecting and communicating any information furnished by or to Customer. No promise, statement, representation or Addendum made by any employee or other representative of MAF Background Screening and not expressed in this Addendum shall bind it contractually or otherwise to Customer.

7. Customer agrees to fully support and implement policies that protect the confidential nature of information furnished by and through MAF Background Screening and insure respect for consumers' rights to privacy. Customer will take precautions to restrict the ability to obtain credit information to key personnel; safeguard access to credit software; safeguard access to websites where credit information can be obtained; protect Customer identification and passwords; and will properly destroy hard copies and electronic files of consumer credit information when no longer needed, or as required by law.

8. Customer hereby agrees to comply with all policies and procedures instituted by MAF Background Screening and required by MAF Background Screening' consumer reporting vendors. MAF Background Screening 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 Addendum at any time after notification of a change in policy in the event Customer deems such compliance as not within its best interest.

9. Customer agrees that MAF Background Screening and MAF Background Screening' consumer reporting vendors shall have the right to audit records of Customer that are relevant to the provision of services set forth in this Addendum and all its attachments. Customer further agrees that it will respond within a requested time frame for information requested by MAF Background Screening' consumer reporting vendors regarding information provided by such vendor. Customer understands that such vendor may suspend or terminate access to the vendor's information in the event Customer does not cooperate with any such an investigation.

10. (a). During the term of this Addendum, Customer agrees to comply with all federal, state and local statutes, regulations and rules applicable to it, including, without limitation the FCRA, with any changes enacted to FCRA during the term of this Addendum, the Gramm Leach Bliley Act and its implementing regulations, any state or local laws governing the disclosure of consumer credit information, and any regulations or limitations promulgated by MAF Background Screening' consumer reporting vendors. Without limiting the foregoing, MAF Background Screening may from time to time notify Customer of new additional, updated or new requirements relating to such laws, compliance with which will be a condition of MAF Background Screening' continued provision of the credit information to Customer, and Customer shall utilize training materials to train and educate its employees in proper security procedures consistent with industry standards. In addition, such new requirements might require price increases. Customer agrees to comply with any such new requirements no later than thirty (30) days after it actually receives notice from MAF Background Screening and such requirements shall be incorporated into this Addendum by this reference. Customer understands and agrees that MAF Background Screening may require evidence, including a certification that Customer understands and will comply with applicable laws.

(b). Customer will implement strict security procedures designed to ensure that Customer's employees use the services and information in accordance with this Addendum and for no purposes other than as permitted by this Addendum. Customer will treat and hold the services and the credit information in strict confidence and will restrict access to the services and the credit information to Customer's employees and customers who agree to act in accordance with the terms of this Addendum and applicable law. Customer will not forward or share information from MAF Background Screening' consumer reporting vendors with any third party. Customer will inform Customer's employees and customers to whom any credit information is disclosed of the provisions of this Addendum. Customer agrees to indemnify MAF Background Screening and its consumer reporting vendors for any claims or losses incurred by MAF Background Screening or its consumer reporting vendors as a result of the misuse of the services or the credit information by Customer or Customer's affiliates, employees, agents, subcontractors or customers in violation of this Addendum.

11. Customer shall notify MAF Background Screening of any 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 within 24 hours following discovery thereof.

12. Customer agrees that MAF Background Screening may verify, through audit or otherwise, that Customer is in fact the end Customer 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. MAF Background Screening may utilize a third party vendor to perform an on-site inspection of Customer's business, and Customer agrees to allow access to such third party.

13. Customer agrees to notify MAF Background Screening of any change of ownership or control fifteen days prior to any such change. MAF Background Screening will require the new ownership to re-apply for the services provided for herein and will require a new physical inspection in the event the office location is changed.

14. Customer hereby authorizes MAF Background Screening to provide copies of any information regarding Customer to MAF Background Screening' consumer reporting vendors.

15. Customer agrees that MAF Background Screening may monitor Customer on an ongoing basis to determine Customer's compliance with applicable law and the provisions of this Addendum. In the event MAF Background Screening determines that Customer is not in compliance with applicable law or this Addendum, Customer's services may be immediately discontinued under this Addendum. Customer shall remain responsible for the payment for any services provided to Customer by MAF Background Screening prior to any such discontinuance.

16. MAF Background Screening will provide, and Customer will utilize, training and training materials to Customer in order for Customer to comply with the federal Fair Credit Reporting Act and with the policies and procedures required by MAF Background Screening's consumer reporting vendors.

17. 15 U.S.C. 1681 *et seq.* also requires certain other responsibilities of Customers of consumer reports from consumer reporting agencies. Those responsibilities are attached (and made a part hereof) as Exhibit A to this Addendum. Customer acknowledges that it is not one of the businesses listed in Exhibit B attached hereto.

18. Customer understands and agrees that basic consumer credit information delivered to Customer by MAF Background Screening is obtained from Trans Union, Equifax Information Services, or Experian Information Solutions, each of which impose different conditions on the acquisition, use and disposal of such information. Customer agrees to abide by the terms and conditions of the attached Appendices A, B and C containing such conditions, which are explicitly made a part hereof.

19. Customer agrees that it will properly dispose of all consumer information. "Consumer Information", as used herein, shall mean any record (or compilation thereof) about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Customer shall comply with all applicable state laws regarding consumer credit or consumer identity protection.

20. Customer shall pay all attorney fees, court costs, ADR fees and collection costs incurred by MAF Background Screening for collecting any delinquent account hereunder, whether or not litigation is instituted. In the event of any litigation or other action involving this Addendum, the prevailing party shall be paid reasonable attorney fees and court costs for trial, appeal, and/or bankruptcy or similar proceeding. In addition, any other recovery to which the prevailing party is entitled shall be paid. If client fails to pay as agreed MAF Background Screening has permission to send a draft for payment to Customer's bank. Customer agrees to pay for all additional services that may be requested through MAF Background Screening

21. Each party to this Addendum is an independent contractor, and nothing contained in this Addendum may be construed as creating a joint venture, partnership, licensor-licensee, principal-agent or mutual agency relationship between or among the parties. No party, by virtue of this Addendum, has any right or power to create any obligation, express or implied, on behalf of any other party. No party, or employee of any party, will be deemed to be an employee of another party by virtue of this Addendum.

22. Customer and MAF Background Screening acknowledge and intend that this Addendum was entered into for the respective benefit of each of them and their respective successors and assigns, and, in consideration of their reporting information to MAF Background Screening, the third party benefit to Trans Union LLC, Equifax Information Services LLC and Experian Information Solutions Inc. Nothing in this Addendum will be construed as giving any other person, firm, corporation or other entity, other than the parties to this Addendum and their respective successors and permitted assigns and Trans Union LLC, Equifax Information Services LLC and Experian Information Solutions Inc., any right, remedy or claim under or in respect of this Addendum or any of its provisions.

23. Due to the special and unique purposes of this Addendum, neither this Addendum nor any rights or obligations in it are assignable by Customer without the prior written consent of MAF Background Screening. Consent will not be unreasonably withheld. Any dissolution, merger, consolidation or other reorganization of Customer, the sale or other transfer of all or substantially all of the assets or properties of Customer, or the sale or other transfer of a controlling percentage of the corporate stock of Customer, constitutes an assignment of this Addendum for all purposes of this paragraph. The term "controlling percentage," for the purpose of this paragraph, means the ownership of stock possessing, and of the right to exercise, at least fifty percent (50%) of the total combined voting power of any class or all classes of stock of such a party, issued, outstanding and entitled to vote for the election of directors, whether that ownership is direct or indirect.

24. Notwithstanding any provision to the contrary, no party to this Addendum will be liable to the other party for any delay or interruption in performance of any obligation resulting from governmental emergency orders, judicial or governmental action, emergency regulations, sabotage, riots, vandalism, labor strikes, or disputes, acts of God, fires, electrical failure, major computer hardware or software failures, equipment delivery delays, acts of third parties, or any other cause, if the delay or interruption in performance is beyond its reasonable control.

25. In the event any provision of this Addendum is held invalid or unenforceable by any court of competent jurisdiction, that holding will not invalidate or render unenforceable any other provision of this Addendum.

26. Failure of any party to enforce any of its respective rights or remedies hereunder with respect to any specific act or failure to act of any party will not constitute a waiver of the rights of that party to enforce those rights and remedies with respect to any other or subsequent act or failure to act.

27. This Addendum, including the Appendices and Exhibits hereto, which are expressly incorporated into it, constitutes the entire Addendum between the parties. No changes in this Addendum may be made except in writing signed by both parties.

28. 15 U.S.C. 1681 *ET SEQ.* PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, UNITED STATES CODE, IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.

29. This Addendum shall be governed by and construed under the laws of the State of _____.

30. The person signing below on behalf of Customer certifies that he/she has direct knowledge of the facts herein and certifies that they have read, understand and will comply with all requirements as set forth in the MAF Background Screening Application for Services, Addendum A and all Exhibits and Appendices which are explicitly made a part hereof

DATED this _____ day of _____, 20____.

| | |
|----------------------|--------------------------|
| _____ | MAF Background Screening |
| CUSTOMER | |
| _____ | _____ |
| Authorized Signature | Authorized Signature |
| _____ | _____ |
| Title | Title |
| _____ | _____ |
| Street Address | Street Address |
| _____ | _____ |
| City State Zip | City State Zip |

Please sign and fax this page and the following completed page to (813)-277-3660

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.

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

The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Federal Trade Commission's Website at www.ftc.gov/credit. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Commission's Web site. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)

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

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

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

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

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

3. Adverse Actions Based on Information Obtained From Affiliates

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

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

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

E. Users Have Obligations When Notified of an Address Discrepancy

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

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The Federal Trade Commission, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Federal Trade Commission's regulations may be found at www.ftc.gov/credit.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must

provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) (“Notice to the Home Loan Applicant”).

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

A. Employment Other Than in the Trucking Industry

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

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- **Before** taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer’s rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

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

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

B. Employment in the Trucking Industry

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

company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the

medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in regulations issued by the banking and credit union regulators) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

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

In addition, once the Federal Trade Commission by rule has established the format, type size, and manner of the disclosure required by Section 615(d), users must be in compliance with the rule. The FTC's regulations will be at www.ftc.gov/credit.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source 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.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

The FTC's Web site, www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

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

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

Exhibit B

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

EXAMPLE LETTER OF INTENT

Letter to be submitted on company letterhead and signed by an Officer or authorized agent for the company

Letter of Intent

Elder Care, Inc.
111 Main St.
Anywhere, US 99999

Elder Care, Inc. is an assisted living facility for adults. We intend to use credit information for the purpose of background screening on prospective employees. We estimate our monthly volume to be 50 reports per month. We have facilities in 35 states and therefore we anticipate our access to be on a national level.

Signed
Mary Smith
President

EXAMPLE LETTER OF INTENT

Letter to be submitted on company letterhead and signed by an Officer or authorized agent for the company

Letter of Intent

Castle Woods, Inc.
111 Main St.
Anywhere, US 99999

Castle Woods, Inc. is property management company. We intend to use credit information for the purpose of screening prospective applicants. We estimate our monthly volume to be 50 reports per month. We have properties in 35 states and therefore we anticipate our access to be on a national level.

Signed
Mary Smith
President

Access Security Requirements

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

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

1. Implement Strong Access Control Measures

- 1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Subscriber Code password be changed immediately when:
 - any system access software is replaced by another system access software or is no longer used;
 - the hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
 - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
 - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 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 your membership application.

- 1.13 Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

- 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, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- 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 Computer Virus detection/scanning product on all computers, systems and networks.
 - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
 - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
 - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
 - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
 - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

3. Protect Data

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- 3.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement 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 credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

4. Maintain an Information Security Policy

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 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.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

5. Build and Maintain a Secure Network

- 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 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

6. Regularly Monitor and Test Networks

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to

access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

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

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

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

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. |
| SSID | Part of the Wi-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part of that network. Wireless devices that communicate with each other share the same SSID. |
| Subscriber Code | Your seven digit credit reporting agency account number. |
| WEP Encryption | (Wired Equivalent Privacy) A part of the wireless networking standard intended to provide secure communication. The longer the key used, the stronger the encryption will be. Older technology reaching its end of life. |
| WPA | (Wi-Fi Protected Access) A part of the wireless networking standard that provides stronger authentication and more secure communications. Replaces WEP. Uses dynamic key encryption verses static as in WEP (key is constantly changing and thus more difficult to break than WEP). |