Thank you for choosing Premium Credit Bureau for your credit reporting needs! As a part of the account setup process, the following items are REQUIRED in order to keep in compliance with the FCRA (Fair Credit Reporting Act) and the three credit bureaus (Transunion, Experian & Equifax).

1. Copy of the current Corporate or Business License.

2. Copy of the front page of a phone or utility bill, indicating the company name and address.

3. Copy of the responisble administator driver's license/identification card.

4. Copy of VOIDED business check.

5. Company letter of intent (sample included)

6. Sample of template of consumer authorization

The final step in the account setup process is the scheduling and completion of an onsite inspection at your office location. A $175 fee will be charged to cover both the onsite inspection and compliance fee for the current year.

Additionally there will a yearly compliance fee of $100.00.

When performing the inspection, the inspector will be looking for the below items:

- **Permanent sign displaying the business name.**
- **Lockable filing cabinet.**
- **Shredder or shredding service.**
- **Indications the business is active.**

If you have any questions or concerns, please contact Premium Credit Bureau at 800-322-8825.

PLEASE E-MAIL REQUIRED DOCUMENTS AND COMPLETED AGREEMENT TO imanzo@pcbscore.com
www.PremiumCreditBureau.com

Revised 04/2019

PREMIUM CREDIT BUREAU SERVICE AGREEMENT

General Company Information

Company Name: _____ Yrs. In Business: Yrs: ____ Mos: ____

Billing/Mailing Address: _____ Phone: _____

Physical Address: _____ Fax: _____

(NO P.O. Box Numbers will be accepted)

City: _____ State: _____ Zip Code: _____ Website Address: _____

Contact Name: _____ E-Mail: _____

Do you own or lease the building in which you are located? ☐ Own ☐ Lease

Type of Business: ☐ Other: _____

Type of Ownership (select one): ☐Partnership ☐Corporation ☐Sole Proprietor ☐Non-profit

Other business name(s), or D.B.A..: _____

Permissible Purpose Information (application will not be processed unless this information is provided.)

Describe the specific purpose for which the credit information provided will be used:

☐Employment

GLB MATRIX: ☐ Pre-employment

How did you hear about us? ☐Advertisement ☐Telephone ☐Directory ☐Referral Sales Call ☐Internet

☐Trade Show ☐Other: _____

Do you own or operate any other business? ☐ Yes ☐ No If Yes, Buiness name: _____

Principal of the Company

Principal's Name:_____ Social Security # _____

Residence: _____ City/State/Zip: _____

Title or Position:_____ Phone: _____

(I understand that the information provided will be used to obtain background check, OFAC report and my creditworthiness may be considered when making a decision to grant services.)

Bank References (or attach copy of voided check from business checking account) **MUST HAVE TO PROCESS**

Bank Name: _____ Contact Name:_____

Address / City / State / Zip: _____

Phone: _____ Business Checking Account # _____

Payment/Billing Method

Client agrees upon receipt of statement for the services rendered during the previous month, according to the current pricing schedule in effect; payments will be due in terms described on the invoice. Past due amounts shall accrue interest at the rate of 1.5% per month. If collection efforts are required, Client shall pay all costs of collection including, but not limited to, attorney's fees. Any returned NSF checks would impose a $30.00 per incident fee to the next statement. Any account with a past due balance over 10 days will be turned off for services. Client shall also pay a $25.00 per incident charge if account has been turned off for past due payment. I understand that if I fail to pay my monthly invoice by the due day the full amount will be deducted from my business or personal checking account or from my business or personal credit/debit card. I further understand that while I retain the right to dispute invoiced amounts; I will not delay the payment in any manner but will accept any account credits on future invoices. I further declare that I am an authorized signer of said account and am authorized by corporate charter or otherwise to enter into this agreement.

Automatic Withdrawl from Checking Account

Bank Account Type _____

Bank Account # _____

Bank Routing # _____

Automatic Withdrawl Credit Card. *(Additional Fees May Apply)

Name on Card _____ Card Type: ☐ Visa ☐ AMEX

Billing Address _____ ☐ Mastercard ☐ Discover

Credit Card # _____ Expiration Date _____ CSV # _____

Signature of officer or authorized representative in this contract is reposible for print of the company invoices every month for internal control. Premium Credit Bureau may provide an electronic billing (Via E-Mail Format).

_____ Email Address to be sent to: _____

(Signature of Officer or Authorized Representative)

or

_____

(Digital Signature of Officer or Authorized Representative

Premium Credit Bureau (PCB) Service Agreement

The Undersigned Applicant (hereinafter referred to as the "Client" agrees):

1. To comply with all the provisions of Public Law 91-508 (Fair Credit Reporting Act (FCRA)) and all other applicable statutes. Client has received the FCRA Addendum.

2. To certify that consumer inquiries will be made, and/or consumer reports ordered only for the permissible purpose as identified in this contract.

3. To certify that all applicants, on which requests will be made for credit information, have signed a form and/or given consent authorizing Client to investigate their credit histories. Client understands that PCB may request from time to time copies of proof to verify such consent on files ordered through PCB. Client also understands that when ordering a Residential Mortgage Credit Report, a full and complete application (1003) is required.

4. To certify that any consumer inquiries/reports will not be used for any form of credit counseling, credit repair or restoration.

5. That any of their employees are forbidden to attempt to obtain reports on themselves, family members, and associates or on any other person, except in the exercise of their official duties.

6. That PCB shall use good faith in attempting to obtain credit information from sources deemed reliable, but does not guarantee the accuracy of the information reported. In no event shall PCB be held liable in any manner whatsoever for any loss or injury to the client resulting from the obtaining or furnishing of such information. Furthermore, that the client agrees to hold PCB and i t s sources (primarily Trans Union, Equifax and Experian) harmless and indemnify them from any and all claims arising out of alleged liability or failure, or error of omission.

7. That with just cause, such as delinquency or violation of the terms of this contract or a legal requirement, PCB may, upon its election, discontinue serving the Client and cancel this Agreement immediately.

8. The Client has read the Score Addendum, Rapid Risk Score Agreement, Flood Certification Agreement, Fannie Mae Addendum, Internet Agreement/Employee Requirements, and Personal Guarantee provided by PCB, and agrees to comply with their provisions when obtaining these services.

9. To authorize PCB to investigate the references, statements and other data contained in this application or obtained from client or any other person pertaining to client's credit responsibility. Client will furnish other information if requested. It is understood that all information obtained will only be used by PCB to evaluate the application and will be held in the strictest confidence.

10. The Client or End User understands they are not to resell the information in whole or in part to any third party.

Client certifies that they have read and accepted all of the above statements and that all of the information provided is accurate.
All replications of this Service Agreement shall be deemed an original.

ADDENDUM FOR OFAC ADVISOR

Premium Credit Bureau, a Florida Corporation with its principal place of business at 2701 E Atlantic Blvd 2nd Floor, Pompano Beach, FL 33062 (Premium Credit Bureau) and _____ ("Client"), having entered into one or more agreements for consumer reporting services and/or ancillary products (collectively "Master Service Agreement).Premium Credit Bureau agrees to make available as an add-on to consumer reports and as an add-on to certain ancillary products offered by Premium Credit Bureau from time to time an indicator whether the consumer's name appears on the United States Department of Treasury Office of Foreign Asset Control File ("OFAC File"). The service is referred to as OFAC Advisor. Client may receive the OFAC Advisor service under the following terms:

$1.00 additional per OFAC inquiry. In the event Client obtains OFAC Advisor services from Premium Credit Bureau in conjunction with Consumer Report or as an append to an ancillary service, Client shall be solely responsible for taking any action that may be required by federal law as a result of a match to the OFAC File, and shall not deny or otherwise take any adverse action against any consumer based solely on Premium Credit Bureau's OFAC Advisor services.

This addendum shall become effective on _____ and remain in effect until cancelled by either party upon written notice to the other. In all other respects, the Agreement shall remain in full force and effect.

ADDENDUM E
Death Master File Certification

Access to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, fiduciary duty, as such business purposes are interpreted under 15 C.F.R § 1110.102 (a)(1).

The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102 (a)(1). As many Experian services contain information from the DMF, Experian would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the Experian services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with your applicable Fair Credit Reporting Act (15 U.S.C. § 1681 et seg.) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) use. Your continue use of Experian services affirms your commitment to comply with these terms and all applicable laws.

You acknowledge you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian services.

COMPREHENSIVE INFORMATION SECURITY PROGRAM

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

ADDENDUM TO AGREEMENT FOR INTERNET SERVICE

The term "credit reports" is used in this Addendum with the meaning assigned to such term in the Agreement.

RECITALS

A. Client desires to obtain credit reports from Premium Credit Bureau through the Internet pursuant to this Addendum.

B. Premium Credit Bureau is willing to furnish credit reports to the Client through the Internet based upon Client's representations, warranties, and covenants in this Addendum.

In consideration of the mutual covenants set forth therein, the parties agree as follows:

1. Orders for and Delivery of Credit Reports. Premium Credit Bureau will accept orders for credit reports from Client transmitted to Premium Credit Bureau at Premium Credit Bureau's Internet Website (WWW.PREMIUMCREDITBUREAU.COM), and Premium Credit Bureau will transmit credit reports ordered by Client in such manner to a location at Premium Credit Bureau's Website that is accessible only pursuant to the subscriber number and password assigned to Client by Premium Credit Bureau (together, "Premium Credit Bureau Password"). Orders for credit reports must include the name, social security number, and address of the subject of the credit report, and any other information specified by Premium Credit Bureau. The operator must have a unique Internet identification and password. **Sharing the identification and password is strictly prohibited.** All credit reports delivered by Premium Credit Bureau to Client through the Internet pursuant to this Addendum will be encrypted.

2. Client agrees to establish and maintain the following security procedures to prevent unauthorized access to credit reports delivered pursuant to this Addendum:

a. Client will protect the Premium Credit Bureau Password so that only authorized employees of Client ("Authorized Employees") have access to this information. Client agrees to limit Authorized Employees to those employees who have a need to know the Premium Credit Bureau Password to carry out their official duties with Company.

Prior to providing an Authorized Employee with access to the Premium Credit Bureau Password, Client will provide the Authorized Employee with adequate training regarding the requirements set forth in Exhibit A attached to this Addendum ("Employee Requirements"). Client agrees not to add any employee as an Authorized Employee unless the employee receives the required training and agrees to comply with the Employee Requirements. Client will be responsible for any failure of an Authorized Employee to comply with any of the Employee Requirements, and Client's indemnity pursuant to Section 7 below shall apply to any such failure to comply. Client will not post the Premium Credit Bureau Password at its facilities, and Client will take all other actions necessary to prevent unauthorized persons from gaining knowledge of the Premium Credit Bureau Password. The Premium Credit Bureau Password must not be released by telephone to any telephone caller, even if the caller claims to be a Premium Credit Bureau employee. The Password can only be delivered to the company e-mail address; therefore it is a requirement of this Addendum for all customers to have a valid business e-mail address. Premium Credit Bureau reserves the right to change the Premium Credit Bureau Password at any time to prevent unauthorized access to credit reports delivered to Client through the Internet.

b. All Internet access software used by Client to order and obtain credit reports through the Internet, whether developed by Client or purchased from a third-party vendor, must have the Premium Credit Bureau Password "Hidden" or embedded so that the Premium Credit Bureau Password is known only to Authorized Employees. Each Authorized Employee must be assigned a unique logon code ("Logon Code") to be able to open and use the Premium Credit Bureau Website. Authorized Employees will be required to protect the secrecy of their Logon Codes, and as soon as an Authorized Employee loses such status (whether by termination of employment or otherwise), CLIENT WILL IMMEDIATELY disable such employee's Logon Code.

c. Client will also follow the security procedures required under the Agreement and agrees to establish such additional security procedures as may be specified by Premium Credit Bureau from time to time. In addition, Client agrees to follow the security and other requirements imposed by Premium Credit Bureau's credit information providers ("Repositories"), as furnished to Client by Premium Credit Bureau from time to time.

3. Client must use Microsoft Internet Explorer version 10.0 and above that supports 128-bit encryption. Client must also have Adobe Acrobat version 10.0 and above **installed.**

4. Client understands and agrees that this Addendum applies only to the delivery of credit reports by Premium Credit Bureau to Client by means of the Internet, and nothing in this Addendum modifies or supersedes the requirements of the Agreement regarding the transfer of credit reports (or any information therein) by Client through the Internet. **Client reaffirms that it will not transmit any credit reports (or information therein) through the Internet without express written permission of Premium Credit Bureau pursuant to the requirements of the Agreement.**

5. **Client agrees that it will permit the Repositories to audit Client's compliance with the requirements of this Addendum and to make any changes required by a Repository. Client agrees that Premium Credit Bureau may terminate or suspend providing credit reports to Client through the Internet pursuant to Section 6 below, if required by a Repository.**

6. Clients agrees that Premium Credit Bureau may change rates without notification, our rates may vary depending on monthly volume, without any liability being incurred by PCB, Premium Credit Bureau may terminate or suspend Client's receipt of credit reports via the Internet at any time, effective immediately on oral or written notice, for any reason including, without limitation, Premium Credit Bureau's determination that such method of transmission to Client imposes a risk of misuse of the credit reports, Client's breach of any requirement of this Addendum or the Service Agreement, any material increase to Premium Credit Bureau in the cost of using the Internet, or any other reason. In addition, if the agreement is terminated, this Addendum shall automatically terminate.

7. Client agrees that its indemnity in the Agreement applies to any breach by Client of its obligations in this Addendum or any misuse of any credit report obtained through the Premium Credit Bureau's Website or any information contained in any such report by any employee of Client, agent, or independent contractor of Client (or former employer, agent, or Independent contractor).

8. Client agrees that Premium Credit Bureau may audit Client's compliance with the requirements of this Addendum at any time on reasonable notice to Client and that Client will cooperate with Premium Credit Bureau in such audits. Client agrees to implement any change to its procedures (whether as a result of such audit or otherwise) and to establish any new procedures requested by Premium Credit Bureau.

9. This Addendum will not be effective until accepted and approved by Premium Credit Bureau. No change in this Addendum may be made except pursuant to a written instrument executed by the Compliance Officer or other authorized officer of Premium Credit Bureau.

EXHIBIT A

EMPLOYEE REQUIREMENTS

All authorized Employees must agree to comply with the following requirements:

1. The employee must have read the portions of the Addendum and the Agreement for Service relating to the permissible purposes for which credit reports may be ordered from Premium Credit Bureau and the restrictions on the use and dissemination of such reports and the information therein, must be familiar with the requirements specified therein, and must agree to comply with such requirements.

2. The employee must agree not to disclose the Premium Credit Bureau Password or the Logon Code assigned to the employee to any other person.

3. The employee must agree not to order credit reports from Premium Credit Bureau except in performance of the employee's official duties for Company. The employee must acknowledge his or her awareness that the Fair Credit Reporting Act provides that **"[any] person who knowingly and willfully obtains information on a consumer from a consumer reporting agency [such as Premium Credit Bureau] under false pretenses shall be fined under Title 18 United States Code, imprisoned for not more than 2 years, or both."**

4. The employee must acknowledge that credit reports contain extremely sensitive information, and agree to protect the privacy of such information by using credit reports obtained from Premium Credit Bureau solely in connection with the employee's official duties for Company, not copying such credit reports (except as required by the employee's official duties), not providing such credit reports or any information therein to any person (except in the course of the employee's official duties), and taking adequate steps to prevent unauthorized persons gaining access to such reports or information.

5. The employee must agree that after termination of his or her employment by Company or Company's withdrawal of the employee's designation as an Authorized Employee, the employee will not obtain or attempt to obtain credit reports from Premium Credit Bureau through the Premium Credit Bureau Password or the employee's Logon Code for any reason.

6. Any scores obtained from the repositories shall not be disclosed to the consumers or any third party unless clearly required by law.

I am requesting the following employees receive user names (passwords will be issued at time of setup). I certify that each employee has read and understands the Exhibit A" as a requirement to access credit reports. Appear on the User for Internet Delivery form.

Users for Internet Delivery

I have signed an Agreement for Internet Service with Premium Credit Bureau. I am requesting the following users from my office to have Internet access to credit reports provided by Premium Credit Bureau. I am requesting the following employees receive user names and passwords. I have given each user shown below a list of the Employee Requirements pertaining to Internet credit reports. I acknowledge that it is my responsibility to contact Premium Credit Bureau if an employee should no longer have access to the credit reports.

Primary Contact Person: _____
(Will use company e-mail address given below)

Secondary Contact Person: _____

Secondary Contact Email Address : _____
(These are officers authorized to make changes to the account)

Each user will need to be designated a title so that we may properly set them up on your account.
Managers will be designated with the letter **"M"** for a **Title** and will have all abilities.

- The ability to view all user reports
- The ability to see all invoices
- The ability to order reports and supplements for all users

Processors (P) - Less the ability to see all invoices.
Loan Officers (L) - will only have the ability to request reports and supplements for
Accountants (A) - will only have the ability to print monthly billing. themselves.
An administrator/manager email address is required. All Internet account billing and correspondence will be sent only to the administrator/manager.

Company E-Mail Address: _____ **(Required)**

Employee Full Name and Title

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

Appendix A
MULTI BUREAU AGREEMENT ADDENDUM

User hereby agrees to comply with all policies and procedures instituted by CRA and required by CRA's consumer reporting vendor. CRA will give User 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. User may terminate this agreement at any time after notification of a change in policy in the event User deems such compliance as not within its best interest.

User agrees that CRA's consumer reporting vendor shall have the right to audit records of User User that are relevant to the provision of services set forth in this Agreement. User further agrees that it will respond within a requested time frame for information requested by CRA's consumer reporting vendor regarding information provided by such vendor. User understands that such vendor may suspend or terminate access to the vendor's information in the event User does not cooperate with such an investigation.

User understands and agrees that, notwithstanding the fact that under federal law User may have several permissible purposes to obtain consumer reports, User shall only obtain such reports in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer. The federal Fair Credit Reporting Act 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 State Code, imprisoned for not more than 2 years, or both."

a. During the term of this Agreement, User 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 Agreement, 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 CRA's consumer reporting vendor. Without limiting the foregoing, CRA may from time to time notify User of additional, updated or new requirements relating to
such laws, compliance with which will be a condition of CRA's continued provision of the credit information to User, and User 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. User agrees to comply with any such new requirements no later than thirty (30) days after it actually receives notice from CRA and such requirements shall be incorporated into this Agreement by this reference. User understands and agrees that CRA may require evidence, including a certification that User understands and will comply with applicable laws. B. User will implement strict security procedures designed to ensure that User's employees and customers use the services and the credit information in accordance with this Agreement. User 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 User's employees and customers who agree to act in accordance with the terms of this Agreement and applicable law. User will inform User's employees and customers to whom any credit information is disclosed of the provisions of this Agreement. User agrees to indemnify CRA for any claims or losses incurred by CRA as a result of the misuse of the services or the credit information by User or User's affiliates, employees, agents, subcontractors or customers in violation of this Agreement.

b. User shall notify CRA 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. b. in the event of such a breach, User agrees to cooperate with CRA and with CRA's consumer reporting vendor in any investigation relating thereto. The nature and timing of any notifications required herein shall be under the control of CRA's consumer reporting vendor, unless otherwise required by law.

c. For purposes of this Agreement, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

d. For purposes of this Agreement, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

e. For purposes of this Agreement, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

f. For purposes of this Agreement "notice" may be provided by one of the following methods: (1) Write notice. (2) Electronic

notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United State Code. (3) E-mail notice when the User has an e-mail address for the subject persons. (4) Conspicuous posting of the notice on the web site of the user.

g. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

h. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

i. In the event the breach is determined by CAR's consumer reporting vendor to be within the control of User, (1) User shall provide to each affected or potentially affected consumer, credit history monitoring services for a minimum of one 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 of the national consumer credit reporting bureaus, and (2) CRA's consumer reporting vendor and CRA may assess User an expense recovery fee.

If approved by CRA and CRA's consumer reporting vendor, User may deliver the consumer credit information to a third party, secondary user which User has an ongoing business relationship for the permissible use of such information. CRA's consumer reporting vendor may charge a fee for the subsequent delivery to secondary users.
User agrees that CRA may verify, through audit or otherwise, that User is in 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.

User agrees to notify CRA of any change of ownership or control fifteen days prior to any such change CRA may require the new ownership to re-apply for the services provided for herein and may require a new physical inspection in the event theoffice location is changed. User hereby authorizes CRA to provide copies of any information regarding User to CRA's consumer reporting vendor. User agrees that CRA may monitor User on an ongoing basis to determine User's compliance with applicable law and the provisions of this Agreement. In the event CRA determines that User is not in compliance with applicable law or this Agreement.
User may immediately discontinue services under this Agreement. User shall remain responsible for the payment for any services provided to User by CRA prior to any such discontinuance.

CRA will provide, and User will utilize, training and training materials to User in order for User to comply with the federal Fair Credit Reporting Act and with the policies and procedures required by CRA's consumer reporting vendor.

APPENDIX A-1

Equifax Requirements

Customer, in order to receive consumer credit information from Equifax Information Services, LLC, through PCB 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 PCB is specifically conditioned upon Customer's agreement with the provisions set forth in this Agreement. Customer understands and agrees that these requirements pertain to all of its employees, managers and owners and that all persons having access to Equifax consumer credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

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

2. Customer certifies that it will order and use Limited-ID or Limited DTEC reports in connection with only one of the following purposes involving the subject of the report and for no other purpose: (a) to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability; (b) for required institutional risk control or for resolving consumer disputes or inquiries; (c) due to holding a legal or beneficial interest relating to the consumer; (d) as necessary to effect, administer, or enforce a transaction to underwrite insurance at the consumer's request, for reinsurance purposes or for the following purposes related to the consumer's insurance: account administration, reporting, investigation fraud prevention, premium payment processing, claim processing, benefit administration or research projects; (e) to persons acting in a fiduciary or representative capacity on behalf of, and with the consent of, the consumer or (f) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, including location for collection of a delinquent account. Customer, if a government agency, certifies it will order and use Limited-ID or Limited DTEC in connection with the following purposes involving the subject and for no other purpose: (y) pursuant to FPCB Section 608 or (z) for an investigation on a matter related to public safety. 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 Customer will riot 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 FPCB, for which a consumer reporting agency is permitted to furnish a consumer report. Equifax may periodically conduct audits of Customer regarding its compliance with the FPCB and other certifications in this Agreement. Audits will be conducted by mail whenever possible and will require Customers to provide documentation as to permissible use of particular consumer, Limited ID, or Limited DTEC reports. Customer gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Customer's material breach of this Agreement, constitute grounds for immediate suspension of service or, termination of this Agreement notwithstanding Paragraph 6 above. If Equifax terminates this Agreement due to the conditions in the preceding sentence, Customer (i) unconditionally releases and agrees to hold EQUIFAX harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

3. Customer certifies that it is not a reseller of the information, a private detective, bail bondsman, attorney, credit counseling firm, financial counseling firm, credit repair clinic, pawn shop (except companies that do only Title pawn), check cashing company, genealogical or heir research firm, dating service, massage or tattoo service, business that operates out of an apartment, an individual seeking information for his private use, an adult entertainment service of any kind, a company that locates missing children, a company that handles third party repossession, a company seeking information in connection with time shares or subscriptions, a company or individual involved in spiritual counseling or a person or entity that is not an end-user or decision maker, unless approved in writing by Equifax.

4. Customer agrees that Equifax shall have the right to audit records of Customer that are relevant to the provision of services set forth in this agreement. Customer authorizes PCB 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 PCB to suspend or terminate access to Equifax's information in the event Customer does not cooperate with any such an investigation. Customer shall remain responsible for the payment for any services provided to Customer prior to any such discontinuance.

5. Equifax information will be requested only for Customer's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted by law. Customer agrees that Equifax information will not be forwarded or shared with any third party unless required by law or approved by Equifax. If approved by Equifax and authorized by the consumer, Customer may deliver the consumer credit information to a third party, secondary, or joint user with which Customer has an ongoing business relationship for the permissible use of such information. Customer understands that Equifax may charge a fee for the subsequent delivery to secondary users. Only designated representatives of Customer will request Equifax information

on Customer's employees, and employees will be forbidden to obtain reports on themselves, associates or any other persons except in the exercise of their official duties. Customer will not disclose Equifax information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax. Customer will hold Equifax and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax information by Customer, its employees or agents contrary to the conditions of this paragraph or applicable law.

6. Customer understands that it must meet the following criteria: (a) the Customer company name, including any DBA's, and the address on the Customer Application ("Application") and Agreement must match; (b) the telephone listing must be verified in the same company name and address that was provided on the Application and Agreement; (c) a copy of the current lease of the business must be reviewed by PCB 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 PCB for valid substitutions when a license is not required by the state), and (f) an on-site inspection of the office is to be conducted by an Equifax certified company. **Note (c) and (d) are not required if the Customer is publicly traded on a nationally recognized stock exchange.*

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

8. Customer agrees that it will properly dispose of all consumer information in accordance with the following. As used herein, "consumer information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data. "Dispose," "disposing," or "disposal" means: (1) the discarding or abandonment of consumer information, or (2) the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored. A Customer who maintains consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Reasonable measures include (1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed; (2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed; and (3) after due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with the above.

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

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

11. Fair Credit Reporting Act Certification. Customer certifies that it will order Equifax Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FPCB"), only when Customer intends to use that consumer report information: (a) in accordance with the FPCB and all state law counterparts; and (b) for one of the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor or services, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation;

(iv) when Customer otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer, or to review an account to determine whether the consumer continues to meet the terms of the accounts; or (v) for employment purposes; provided, however, that CUSTOMER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYMENT PURPOSES UNLESS CUSTOMER HAS A SUBSCRIPTION TO THE EQUIFAX PERSONA SERVICE. Customer will use each consumer report ordered under this Agreement for one of the foregoing purposes and for no other purpose. It is recognized and understood that the FPCB provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency (such as Equifax) under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Customer regarding its compliance with the FPCB and other certifications in this Agreement. Audits will be conducted by mail whenever possible and will require Customers to provide documentation as to permissible use of particular consumer, Limited ID, or Limited DTEC reports. Customer gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Customer's material breach of this Agreement, constitute grounds for immediate suspension of service or, termination of this Agreement notwithstanding Paragraph 6 above. If Equifax terminates this Agreement due to the conditions in the preceding sentence, Customer (i) unconditionally releases and agrees to hold EQUIFAX harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

California Law Certification

Customer will refer to Appendix A-4 in making the following certification, and Customer agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.

Vermont Certification

Customer certifies that it will comply with applicable provisions under Vermont law. In particular, Customer certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFPCB"), only after Customer has received prior consumer consent in accordance with VFPCB Section 2480e and applicable Vermont Rules. Customer further certifies that the attached copy of Section 2480e (Exhibit 1-B) of the Vermont Fair Credit Reporting Statute was received from EQUIFAX. Customer will comply with the applicable provisions of the FPCB, Federal Equal Credit Opportunity Act, Gramm-Leach-Bliley Act and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer.

12. This Section 12 applies to any means through which Customer orders or accesses the Information Services including, without limitation, system-to-system, direct access terminal, personal computer or the Internet; provided, however, Customer will not order or access the Information Services via the Internet without first obtaining Equifax's written permission. For the purposes of this Section 9, the term "Authorized User" means a Customer employee that Customer has authorized to order or access the Information Services and who is trained on Customer's obligations under this Agreement with respect to the ordering and use of the Information Services, and the information provided through same, including Customer's FPCB and other obligations with respect to the access and use of consumer reports. Customer will: (a) ensure that only Authorized Users can order or have access to the Information Services and the information provided through same, (b) ensure that Authorized Users do not order credit reports for personal reasons or provide them to any third party, (c) ensure that all devices used by Customer to order or access the Information Services are placed in a secure location and accessible only by Authorized Users and that these devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures, and (d) take all necessary measures to prevent unauthorized ordering or access to the Information Services by any persons other than Authorized Users for permissible purposes. Those measures will include, without limitation, limiting the knowledge of the Customer security codes, telephone access number(s) Equifax provides, and any passwords Customer may use, to Authorized Users and other employees with a need to know, changing Customer's user passwords at least every ninety (90) days, or sooner if it is obtained by any third party or an Authorized User is no longer responsible for accessing the Information Services, or if Customer suspects an unauthorized person has learned the password, and using all security features in the software and hardware Customer uses to order or access the Information Services. Customer will monitor compliance with the obligations of this Section 12, and will immediately notify Equifax if Customer suspects or knows of any unauthorized access or attempt to access the Information Services. Such monitoring will include, without limitation, a review of each Equifax invoice for the purpose of detecting any unauthorized activity. Customer will not ship hardware or software between Customer's locations or to third parties without deleting all Equifax Customer number(s), security codes, telephone access number(s) and Customer user passwords. If Customer uses a third party vendor to establish access to the Information Services, Customer is responsible for the third party vendor's use of Customer's member numbers, security access codes, or passwords. Customer will ensure the third party vendor safeguards Customer's security access code(s) and passwords through the use of security requirements that are no less stringent than those applicable to Customer under this Section 9. Customer will inform Authorized Users and other employees with a need to know that unauthorized access to consumer reports may subject them to civil and criminal liability under the FPCB punishable by fines and imprisonment. If Equifax reasonably believes that Customer has violated this Section 12, Equifax may, in addition to any other remedy authorized by this Agreement, with reasonable

advance written notice to Customer and at Equifax's sole expense, conduct, or have a third party conduct on its behalf, an audit of Customer's network security systems, facilities, practices and procedures to the extent Equifax reasonably deems necessary in order to evaluate Customer's compliance with the data security requirements of this Section 12.

APPENDIX A-2

Additional Equifax Information Services

This Appendix A-2 supplements the service agreement ("Agreement") under which Customer receives, as part of its service from PCB, 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 desires to receive the services listed below excepting those where Customer's authorized representative places his or her initials. Customer agrees to abide by the additional terms and conditions that apply to the service(s) so selected.

☐ BEACON ☐ Pinnacle K

☐ SafeScan ☐ PERSONA

☐ North American Link

1- BEACONSM - 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. 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.

(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.

(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 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 general manner 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.

(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.

(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. 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. 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

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

(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.

(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. SAFESCAN®

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. 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. Customer will not use a SAFESCAN alert or warning message in its decision-making process for denying credit or any other FPCB 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. Customer understands that the information supplied by SAFESCAN may or may not apply to the consumer about whom Customer has inquired.

4. 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. FPCB Certification. Customer will notify Equifax whenever a consumer report will be used for employment purposes. 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. 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 FPCB, 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. Customer acknowledges that it has received from Equifax a copy of the written disclosure form prescribed by the FTC.

5. North American Link

(a) Desiring to obtain credit reporting services on residents of the United States and Canada through Equifax's North American Link access mechanism, Customer understands that credit reporting services on residents of Canada will be provided from the credit reporting database of Equifax Canada Inc. Customer further understands that Equifax is merely facilitating access and receipt of credit reporting services from Equifax Canada Inc. and that Equifax has not prepared and is not responsible for the credit reporting services received from Equifax Canada Inc.

(b) Further, Customer acknowledges having received and having read the attached Provincial Legislative Overview for International Customers of Equifax's "North American Link" generally describing some additional requirements of various Canadian provinces regarding the request and use of credit reporting information on residents of those provinces. Customer will comply with applicable provincial laws on consumer credit reporting or on protection of personal information (privacy), including obtaining consent if required, in connection with credit reporting services received from Equifax Canada.

APPENDIX A-3

EQUIFAX REQUIREMENT

VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

The undersigned 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 "VFPCB") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FPCB") and its other state law counterparts. In connection with Customer's continued use of Equifax information services in relation to Vermont consumers, Customer hereby certifies as follows:

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

APPENDIX A-4

State Compliance Matters-California Retail Seller

Section 1785.14(a) of the California ?Civil Code imposes special requirements with respect to transactions in which a "retail seller" (as defined in Section 18-2.3 of the California Civil Code) intends to issue credit to a California resident who appears in person on the basis of an application for credit submitted in person ("point of sale transactions"). Client certifies that these requirements do apply to it because (a) Client is NOT a "retail seller" as defined in Section 1802.3 of the California Civil Code), and/or (b) Client does NOT issue credit to California residents who appear in person on the basis of applications for credit submitted in person. Client further certifies that it will notify PCB in writing 30 days PRIOR to becoming a retail seller or engaging in point of sale transactions with respect to California residents.

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. If Customer designated in Section 8 of the Agreement that it 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. 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.

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

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

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

(2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer. (b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.

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

(1) the ability of a person who has secured the consent of the consumer pursuant to subdivision

(2) of this section to include in his or her request to the consumer permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and (2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

VERMONT RULES *** CURRENT THROUGH JUNE 1999 ***

AGENCY 06. OFFICE OF THE ATTORNEY GENERAL

SUB-AGENCY 031. CONSUMER PROTECTION DIVISION

CHAPTER 012. Consumer Fraud-Fair Credit Reporting

RULE CF 112 FAIR CREDIT REPORTING

CVR 06-031-012, CF 112.03 (1999)

CF 112.03 CONSUMER CONSENT

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and

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

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

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

APPENDIX B
Access Security Requirements for PCB End-Users for FCRA and GLB 5A Data

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

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

1. Implement Strong Access Control Measures

1.1 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from PCB will ever contact you and request your credentials.
1.2 If using third party or proprietary system to access PCB's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing PCB data/systems.
1.3 If the third party or third party software or proprietary system or software, used to access PCB 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 PCB's infrastructure. Each user of the system access software must also have a unique logon password.
1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.
1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.
1.7 Develop strong passwords that are:

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

1.8 Passwords (e.g. 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 algorithm are utilized (e.g. AES 256 or above).
1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30 minute inactive session timeout.
1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of the membership application.
1.13 Company must NOT install Peer\to\Peer file sharing software on systems used to access, transmit or store Experian data.
1.14 Ensure that Company employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
1.15 Implement a process to terminate access rights immediately for users who access Experian credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.
1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.
2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

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

3. Protect Data

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).
3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.
3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.
3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.
3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass\code.
3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.
3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.
3.9 When no longer in use, ensure that hard\copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard\copy materials cannot be reconstructed.
3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry\accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.
4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.
4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. If you believe Experian data may have been compromised, immediately notify PCB within twenty;four (24) hours or per agreed contractual notification timeline (See also Section 8).

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.
4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with 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.

5. Build and Maintain a Secure Network

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

6. **Regularly Monitor and Test Networks**

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)
6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow\up to exceptions is required.
6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access PCB systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

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

7. Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.
7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.
7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.
7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non\secured applications on the mobile device.

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

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

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
    - ISO 27001
    - PCI DSS
    - EI3PA
    - SSAE 16 – SOC 2 or SOC3
    - FISMA
    - CAI / CCM assessment

8. General

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

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to PCB 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 PCB 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 PCB 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 PCB systems shall be made available to PCB upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to PCB 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 PCB within twenty\four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to PCB 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 305\468\1560, Email notification will be sent to imanzo@pcbscore.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 PCB 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 PCB networking and computing resources may be monitored and audited by PCB, without further notice.

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 PCB 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 PCB.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 60 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 60 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."

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 PCB provided services via Internet ("Internet Access").

General Requirements:

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

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with PCB 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 PCB on information and product access, in accordance with these Experian Access Security Requirements for PCBEnd\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 PCB's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to PCB immediately.
2. As a Client to PCB's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to PCB product access control (e.g. request to add/change/remove access). The Company can opt

to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with PCB's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding PCB representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

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

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.
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. EI3PA1 requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA1 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.

END USER CERTIFICATION OF USE FOR EMPLOYMENT INSIGHT REPORTS

In compliance with the Federal Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (the "Act"), _____ ("End User") hereby certifies to Consumer Reporting Agency that it will comply with the following provisions:

1. End User will ensure that prior to procurement or causing the procurement of a consumer report for employment purposes (an Employment Insight Report):

a) a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and

b) the consumer has authorized in writing the procurement of the report by the End User.

2. In using a consumer report for employment purposes, before taking any adverse action based in whole or in part on the report, the End User shall provide to the consumer to whom the report relates

a) a copy of the report; and

b) a description in writing of the rights of the consumer under the Act, a copy of which is attached hereto ("Summary of Consumer Rights").

The information from the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

End User hereby acknowledges receipt of the Summary of Consumer Rights.

_____
(Name of End User)

_____
(Signature)

_____
(Title)

_____
(Date)

Appendix C

GLB ADDENDUM AND ACCESS SECURITY ADDENDUM

We must work together to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of consumer information. In accessing consumer information products, you agree to follow these measures.

1. You must protect your account number and password so that only key personnel employed by your company know this sensitive information. Unauthorized persons should never have knowledge of your password. Do not post this information in any manner within your facility. If a person who knows the password leaves your company or no longer needs to have it due to a change in duties, the password should be changed immediately.

2. System access software, whether developed by your company or purchased from a third party vendor, must have your account number and password "hidden" or embedded and be known only by supervisory personnel. Assign each user of your system access software a unique logon password. If such system access software is replaced by different access software and therefore no longer in use or, alternatively, the hardware upon which such system access software resides is no longer being used or is being disposed of, your password should be changed immediately.

3. Do not discuss your account number and password by telephone with any unknown caller, even if the caller claims to be an employee of your credit provider.

4. Restrict the ability to obtain consumer information products-to a few key personnel.

5. Place all terminal devices used to obtain consumer information products in a secure location within your facility. You should secure these devices so that unauthorized persons cannot easily access them.

6. After normal business hours, be sure to turn off and lock all devices or systems used to obtain consumer information products.

7. Secure hard copies and electronic files of consumer information products within your facility so that unauthorized persons cannot easily access them.

8. Shred or destroy all hard copy consumer information products when no longer needed.

9. Erase and overwrite or scramble electronic files containing consumer information when no longer needed and when applicable regulation(s) permit destruction.

10. Make all employees aware that your company can access consumer information products only for the GLB Exception Appropriate use/Appropriate industry listed on GLB Matrix section of your membership application. You or your employees may not access their own information. Nor should you or your employees' access information of a family member or friend unless it is in connection with an appropriate GLB transaction.

11. The end user acknowledges their responsibility under GLB and will comply.

12. Select the specific appropriate use(s) for which the credit information will be used:
    a) Collection Agency
    b) Pre-employment
    c) Fraud Prevention

Acknowledgment of Service Agreement

I have read and understand the below:

- ☐ Payment/Billing Method
- ☐ PCB Service Agreement
- ☐ Addendum for OFAC Advisor
- ☐ Addendum to Agreement for Internet Service
- ☐ User for Internet Delivery
- ☐ Multi Bureau Agreement Addendum - Appendix A
- ☐ Access Security Requirements - Appendix B
- ☐ End User Certification for Use of Employment Insight Reports
- ☐ GLB Product Addendum - Appendix C
- ☐ Death Master File Addendum - Appendix E / Comprehensive Information Security Program

By signing below you have both read and agree to the contents of this agreement in its entirety and agree to adhere to the above addendums, agreements and billing/payment methods.

_____
Signature

_____
Digital Signature

Name _____

Title _____

Date _____

PCB use only Accepted by:

_____
Signature

_____
Digital Signature

Name _____

Title _____

Date _____

Sample Letter of Intent

ABC Mortgage Company
123 Main Street Los Angeles, California 12345

Date:
To Whom It May Concern:

We at ABC Mortgage Company will use Premium Credit Bureau for the purposes of preapprovals for home buyers for a mortgage loan. We understand that we may not pull credit reports for any other reason. My anticipated monthly volume is **[EST. MONTHLY VOLUME]** reports. I anticipate that our access will be primarily **[LOCAL, REGIONAL or NATIONAL]**.

Sincerely,

Signature

Printed Name Title
