**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 Real Estate, Dept. Of Corporations and/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 responsible administrator driver's license/identification card.*
4. *Copy of VOIDED business check*
5. *Company letter of intent (sample included)*

The final step in the account setup process is the scheduling and completion of an onsite inspection at your office location. A $75 fee will be charged to cover both the onsite inspection and all other setup fee(s).

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****.*

**Businesses operating out of a residential location, will be REQUIRED to have an onsite inspection performed ANNUALY with a yearly fee of $75. Plus other applicable fee(s).*

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

**PLEASE EMAIL COMPLETED APPLICATION & REQUIRED DOCUMENTATION TO SETUP@MYPCBDATA.COM**

**WWW.MYPCBDATA.COM**

# 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: _____

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:

GLB MATRIX: ☐ Collection Agency ☐ Pre-employment ☐ Fraud Prevention

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

Please provide additional information to the above question (i.e. which advertisement, who referred you, sales representative, etc.)

_____

Have you purchased credit reports before? ☐ Yes ☐ No. If yes, from what company? _____

Broker's License #: MLS: # _____ State: _____

**(Please provide a copy of your broker's license when submitting this application)**

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

Kind of Business: _____ Address / City / State / Zip: _____

**Principal of the Company**

Principal's Name: test Social Security #: _____

Residence: _____ City/State/Zip: _____

Title or Position: _____ Phone: ( ____ ) _____

(I understand that the information provided above 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 # _____

**Trade References** (Use title companies, appraisal companies, wholesale lenders, and/or other trade accounts) **MUST HAVE**

Company: _____ Contact: _____ Phone: (____) _____

Company: _____ Contact: _____ Phone: (____) _____

Company: _____ Contact: _____ Phone: (____) _____

# 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 Withdrawal from Checking Account

Bank Account Type _____

Bank Account # _____

Bank Routing # _____

☐ Automatic Withdrawal 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 responsible for print the company invoices every month for internal control. Premium Credit Bureau may provide an electronic billing (Via E-Mail Format).

_____

(Signature of officer or authorized representative) E-Mail Address to be sent to: _____

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 its 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.

# Personal Guarantee

The undersigned individual, being employed by and/or financially interested in the Subscriber identified below, and in consideration of Premium Credit Bureau entering into a service agreement and related contracts ("Agreements") with such Subscriber, personally and individually guarantees all payments due to Premium Credit Bureau by Subscriber under said Agreements. The undersigned waives presentment, protest, demand and notice of dishonor or default in connection with this guarantee and any payments due by Subscriber under the Agreements, and the individual expressly recognizes that this Guarantee creates personal obligation, and that any default under this Guarantee may be reflected on the undersigned" personal credit file. The undersigned further expressly acknowledge the right of Premium Credit Bureau to check the undersigned" personal credit file and/or other financial references.

Printed Name of Individual Guarantor: test

(First) (M.I.) (Last)

Home Address: _____

City, State, and Zip: _____

Social Security #: _____

Phone: (____) ____ _____

Signature: _____ Dated: Thu Feb 26 2015 2

or

Digital Signature: _____

**************IMPORTANT*****************

**In the event that your employment or relationship with the above referenced Subscriber should terminate, it is your responsibility to notify Premium Credit Bureau in writing, so that we may secure another personal guarantor. Otherwise, this Guarantee remains binding against you until Premium Credit Bureau releases you from this Guarantee in writing.**

# Score Addendum

Client ("End User") warrants that is has an agreement for service and an account in good standing with Premium Credit Bureau ("Broker") for a permissible purpose under the Fair Credit Reporting Act to obtain the information in a Fair Isaac Credit Repository Score(s), FICO, Beacon and their reason codes.

End User certifies that all scores and reason codes whether oral or written shall be maintained by the applicant in strict confidence and disclosed only to employees whose duties reasonably relate to the legitimate business purpose for which the report is requested and will not sell or otherwise distribute to third parties any information received there under, except as otherwise required by law.

Unless explicitly authorized in this Agreement or in a separate agreement, between Broker and End User, for scores obtained from credit repository, or as explicitly otherwise authorized in advance and in writing by credit repository through Broker, End User shall not disclose to consumers or any third party, any not all such scores provided under this Agreement, unless clearly required by law. Reason codes may be utilized to assist in preparing an adverse action (denial letter) to consumer.

End User shall comply with all applicable laws and regulations in using the Scores and reason codes.

End User may not use the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of the credit repositories, Fair Isaac and Company, Broker, the affiliates of them or of any other party involved in the provision of the Score without such entities written consent.

End User agrees not in any manner either directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Credit Repository/Fair Isaac in performing the Credit Repository Score.

A requirement that each End User maintain internal procedures to minimize the risk of unauthorized disclosure and agree that such Scores and reason codes will be held in strict confidence and disclosed only to those of its employees with a "need to know" and to no other person;

A provision limiting the aggregate liability of Experian/Fair, Isaac to each End User to the lesser of the Fees paid by Broker to Experian/Fair, Isaac pursuant to Section 3.A of this Agreement for the Experian/Fair, Isaac Model resold to the pertinent End User during the six (6) month period immediately preceding the End User's claim, or the fees paid by the pertinent End User to Broker under the Resale Contract during said six (6) month period, and excluding any liability of Experian/Fair, Isaac for incidental, indirect, special or consequential damages of any kind.

Warranty: Credit Repository, Fair Isaac warrants the Credit Repository Score Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Credit Repository Score Model is applied is similar to the population sample on which the Credit Repository Score Model was developed, Credit Repository Score Model may be relied upon by Broker and/or End Users to rank consumers in order of the risk of unsatisfactory payment such consumers might present to End Users. Credit Repository/Fair Isaac further warrants that so long as it provides the Credit Repository Score Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 et seq. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES CREDIT REPOSITORY/FAIR ISAAC HAVE GIVEN BROKER AND/OR END USERS WITH RESPECT TO THE CREDIT REPOSITORY SCORE MODEL AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED CREDIT REPOSITORY/FAIR ISAAC MIGHT HAVE GIVEN BROKER AND/OR END USERS WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Broker and each respective End User's rights under the foregoing warranty are expressly conditioned upon each respective applicant's periodic revalidation of the Credit Repository Score Model in compliance with the requirements of regulation B as it may be amended from time to time (12 CFR section 202 et seq.)

**RAPID RESCORE REVIEW SERVICE AGREEMENT ADDENDUM**.

1. **Purpose and Scope.** Client is currently using or will be using the services of Premium Credit Bureau as described in the Agreement. Client desires to purchase and Premium Credit Bureau agrees to furnish the Rapid Risk Score Review (the "Service"), as described in materials provided, which is incorporated into and made a part of this Addendum. Accordingly, the parties hereby amend the Agreement with the terms and conditions of the Addendum and agree as follows:

2. **Provision of the Service and Disclaimer.** Premium Credit Bureau agrees to provide the Service to Client, as available, on a non-exclusive basis during the term of the Addendum. It is understood that the Service applies only to information provided to client from the repositories accessed and that Premium Credit Bureau makes no representation or warranty that it can handle every consumer dispute that Client may submit through the Service.

3. **Pricing.** Client agrees to pay for the Service in accordance with the terms of the Service Agreement set forth.

4. **Responsibilities of Client and Premium Credit Bureau.** (A) Client will: (i) assure that all items in dispute submitted through the Service relate to credit repository information; (ii) assure that each such item submitted for the Service has been disclosed to the consumer prior to submission of the dispute; (iii) submit to Premium Credit Bureau for the Service, only those items Client reasonably believes constitutes a valid dispute; (iv) comply with all federal, state and local laws and regulations applicable to Client's use of the Service; (v) make no warranties or guarantees of any kind or nature to the consumer; (vi) communicate the dispute to Premium Credit Bureau in accordance with Premium Credit Bureau's procedures; and (vii) ASSURE THAT ANY COSTS OR FEES PREMIUM CREDIT BUREAU CHARGES CLIENT FOR THE SERVICE WILL UNDER NO CIRCUMSTANCES BE CHARGED BACK TO THE CONSUMER EITHER DIRECTLY OR INDIRECTLY.

(B) XXXXX will perform the Service in accordance with the federal Fair Credit Reporting Act and applicable state law equivalents.

5. **Indemnification.** Client will indemnify and hold harmless Premium Credit Bureau and its directors, officers, and its' employees from and against, of whatever kind or nature and without limitation, any loss, cost, liability, and expense (including reasonable attorney's fees) resulting from Client's, its employee's or agent's acts or omissions related to this Agreement or breach of any obligation under this Agreement.

6. **Limitation of Liability.** Premium Credit Bureau and the repositories involved does not warrant that it can process or resolve any dispute through the Service and except as otherwise expressly provided in this agreement, neither party guarantees or warrants the correctness, merchantability or fitness for a particular purpose of the information or service provided to the other. Information corrected will be reflected on a new Infile credit report only, which needs to be accessed by the Client. NO GUARANTEES ARE MADE ON SCORE REVISIONS.

7. **Term and Termination.** This Addendum will remain in effect until the earlier of (i) the termination of the Agreement or (ii) either party terminates this Addendum by giving not less than ten days prior written notice to the other of its intent to terminate. The obligations of Paragraphs 3, 4, 5 and 6 will survive the termination of this Addendum.

8. **Incorporation and Ratification.** Except to the extent specifically modified by this Addendum., all other terms and conditions of the Agreement remain in full force and effect and are hereby ratified and affirmed by Premium Credit Bureau and Client. The terms of this Addendum constitute the entire understanding of the parties with respect to the subject matter herein, and supersedes all prior agreements or understandings.

9. **Governance in the Event of Conflict.** To the extent of any conflict between the terms of this Addendum and those of the Agreement, the specific terms of this Addendum will control.

# ADDENDUM FOR OFAC ADVISOR

Premium Credit Bureau, a Florida Corporation with its principal place of business at 2412 NW 87 Place, Doral, FL 33172 (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 Thu Feb 26 2015 20:21:: 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
## 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.

# 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. _____

# AGREEMENT FOR SERVICE

**Fannie Mae**

## RECITALS

A. Client desires to receive consumer credit reports including consumer creditworthiness scores ("Credit Reports") and other consumer information (collectively, "Credit Information") through the Fannie Mae MORENETPlus® Network ("Network").

B. Company is willing to provide Client access to the Credit Information through the Network pursuant to the terms of this Agreement. The information contained in the Credit Information is obtained from multiple national consumer credit information repositories and their contractual affiliates ("Repositories"), and is provided as a merged product through a third party vendor ("Vendor").

## AGREEMENT
## SECTION I - CLIENT REQUIREMENTS

In order to obtain Credit Information pursuant to this Agreement, Client agrees to the following requirements, terms, and conditions:
1.1 **Client Eligibility Requirements.** In order to access Credit Information hereunder, Client shall satisfy the following eligibility requirements ("Eligibility Requirements"): Client must (a) be a licensee of Fannie Mae, in good standing and eligible to use Fannie Mae application software accessible via the Network (such as Desktop Underwriter®, Desktop Originator®, and Desktop Home Counselor®), and (b) be a residential mortgage lender or broker, mortgage insurance company, nonprofit mortgage counseling agency, or other entity directly involved in originating mortgage loans. Client represents, warrants, and covenants that it presently satisfies, and throughout the term of this Agreement will continue to satisfy, the Eligibility Requirements, and agrees to immediately notify Company if at any time it ceases to satisfy any of the Eligibility Requirements or, to Client's knowledge, becomes likely to cease to satisfy such requirements.

1.2 In connection with pre-qualification or affordability analyses for taking applications in connection with actual or potential residential mortgage transactions involving the consumer subject of the Credit Information, and for no other purpose. Client will have a limited, nonexclusive license solely to display and use the Credit Information in accordance with the terms of this Agreement and the requirements of applicable law.

1.3 **FCRA.** Client is familiar with the Fair Credit Reporting Act, as amended, ("FCRA), 15 USC 1681 et seq., and is aware that the FCRA provides that anyone **"who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than 2 years, or both."** Client covenants that it will comply with the FCRA and all other applicable federal and state laws with respect to the use of the Credit Information received hereunder.

1.4 **Confidentiality.** Client understands that the Client Information is extremely sensitive and confidential information, and Client agrees to use such information solely for the permissible purposes set forth in Section 1.2 above, to hold all such in strict confidence, and not to sell or otherwise provide such information to any third party. Client agrees further that only authorized employees of Client with a "need to know" and who have received training regarding the FCRA and their obligations under this Agreement will have access to Credit Information. Client agrees that all equipment that Client uses in order to order or receive Credit Information will be placed in a secure location and only authorized employees will have access to such equipment. Client agrees to take all necessary measures to prevent any unauthorized access to, or use of, Credit Information by any person other than Client's authorized employees, and will establish and enforce policies whereby Client's employees are forbidden to obtain or use Credit Information for purposes not permitted under this Agreement or applicable law, and to ensure compliance with all the other requirements of this Section 1.4.

1.5 **Payment Terms.** To pay Premium Credit Bureau upon receipt of statement for the services rendered during the previous month; payments shall be due within 15 days after receipt of 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.

1.6 **Indemnification.** Client agrees to indemnify and hold harmless Company, Vendor, Repositories and all of their respective agents, employees, and independent contractors on account of any demand, action, loss, cost, expense (including, without limitation, reasonable attorney's fees and costs of litigation), damage, liability, penalty or claim (collectively "Claim") arising or resulting in connection with Client's breach of this Agreement, including, without limitation, the improper use, publication, or disclosure of Credit Information contrary to the terms of this Agreement or violation of applicable law by Client or any of its employees, agents, or independent contractors.

1.7 **Disclaimer.** NEITHER COMPANY, VENDOR, NOR ANY REPOSITORY MAKES ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES ARISING FROM A COURSE DEALING OR A COURSE OF PERFORMANCE, WITH RESPECT TO ANY CREDIT INFORMATION OBTAINED HEREUNDER, OR SOFTWARE PROVIDED IN CONNECTION WITH THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, WITH RESPECT TO (A) SUCH CREDIT INFORMATION, ITS ACCURACY, VALIDITY, OR COMPLETENESS OR THAT IT WILL BE PROVIDED ON AN UNINTERRUPTED BASIS, (B) SUCH SOFTWARE, THAT IT WILL BE FREE FROM

ERRORS, AND (C) BOTH, THAT THEY WILL MEET CLIENT'S NEEDS, AND ALL SUCH PERSONS EXPRESSLY DISCLAIM ALL SUCH RESPRESENTATIONS AND WARRANTIES.

1.8 **Release.** Recognizing that Credit Information is created by and through fallible human sources, and that for the fee charged, neither Company, Vendor, nor any Repository can be the insurer of the accuracy, validity, completeness of any Credit Information, Client understands and agrees that the accuracy, completeness, and validity of Credit Information obtained hereunder is not guaranteed by Company, Vendor, or any Repository. CLIENT RELEASES ALL SUCH PERSONS AND THEIR AGENTS, EMPLOYEES, AND INDEPENDENT CONRACTORS FROM ANY AND ALL CLAIMS FOR ANY INACCURACY, INVALIDITY, OR INCOMPLETENESS OF ANY CREDIT INFORMATION PROVIDED HEREUNDER, INCLUDING, WITHOUT LIMITATION, ANY LOSS OR EXPENSE SUFFERED BY CLIENT OR ANY OTHER PERSON RESULTING DIRECTLY OR INDIRECTLY FROM ANY CREDIT INFORMATION PROVIDED HEREUNDER. IN NO EVENT WILL COMPANY, VENDOR, OR ANY REPOSITORY HAVE ANY LIABILITY TO CLIENT OR ANY OTHER PERSON FOR SPECIAL, CONSEQUENTIAL, OR ANY OTHER DAMAGES RESULTING FROM (A) THE INACCURACY, INCOMPLETENESS, OR INVALIDITY OF ANY CREDIT INFORMATION, OR (B) ANY SOFTWARE PROVIDED IN CONNECTION WITH THIS AGREEMENT, EVEN IN THE EVENT THAT COMPANY, VENDOR, OR A REPOSITORY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.9 **Audit.** In order to monitor the Client's compliance with the terms of this Agreement, Client agrees to permit Company, Vendor, and their representatives to conduct reasonable audits from time-to-time of Client's procedures and practices in connection with such compliance. Client agrees to cooperate in connection with such audits and to make available all documents, employees, and information reasonably requested by the auditing party.

1.10 **Force Majeure.** Neither Company, Vendor, nor any other person shall have any liability to Client or any third party for any Claim in connection with any delay, interruption, or failure of performance providing Credit Information hereunder resulting from governmental emergency orders or regulations or judicial or other governmental actions; sabotage, riots, vandalism, labor strikes or disputes; acts of God; Network or other computer hardware or software transmission distortion, interruption, delay, or failure; acts or omissions of Fannie Mae or its agents or other third parties; or any other cause if such cause is beyond its reasonable control. 1.11 **Termination.** Notwithstanding the foregoing, this Agreement shall terminate automatically if Company's agreement with Vendor terminates, and Company may suspend or terminate this Agreement immediately (and Vendor may immediately suspend or terminate providing Credit Information to Client) if Client is in breach of any of its obligations hereunder in connection with ordering or using Credit Information or if Client ceases to satisfy any Eligibility Requirement. In the event of such termination, Client will have no further right to receive Credit Information or use any software provided in connection with this Agreement. The provisions of Sections 1.2, 1.4, 1.6, 1.7, 1.8, and 1.10 above, as well as any payment obligations of Client hereunder outstanding as of the date of termination, shall survive any termination of this Agreement.

1.12 **Third Party Beneficiaries.** Vendor is a third party beneficiary of all obligations of Client to it hereunder, and may enforce such obligations directly, to the same extent as if it were a direct party here to.

**AGREEMENT TO PROVIDE CREDIT INFORMATION**

In reliance on Client's representations, warranties, and covenants in this Agreement, Company agrees to provide Credit Information to Client on the terms and conditions of this Agreement. This Agreement will be effective as of the date it is executed by Company as indicated below.

# Freddie Mac Addendum

I would like to sign up for the Freddie Mac access Premium Credit Bureau. This particular service requires the Freddie Mac TPO, or Seller / Servicer Number given to you from the LP services. I understand that I would still continue to pull LP files through the Freddie Mac website, and with this service a courtesy copy of all LP files will be placed on the Premium Credit Bureau website as well.

My TPO Number: _____

or

Seller / Servicer Number: _____

## 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

# 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 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 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.*

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

## 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.<br>EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian.<br>EI3PA℠ also establishes quarterly scans of networks for vulnerabilities. |
| **ISO 27001 /27002** | IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard)<br>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<br>SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy.<br>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.<br>The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. |

## APPENDIX C
## BUSINESS CREDIT REPORT ADDENDUM

**A. Restrictions on Use.** In consideration for Customer's right to receive and use certain data and services (collectively, the "Services") from Premium Credit Bureau and Experian, Customer understands and certifies to Experian and Premium Credit Bureau that the Services:

(i) will be used solely in connection with a present or prospective credit or financial transaction with the business entity inquired upon or for other legitimate commercial purposes;

(ii) will not be used as a factor in establishing an individual's eligibility for (a) credit or insurance to be used primarily for personal, family or household purposes, or (b) employment;

(iii) will be used in compliance with all applicable laws, regulations and ordinances, and all special use restrictions set forth in the Agreement or adopted by Experian and/or Premium Credit Bureau hereafter; and

(iv) will be maintained in confidence and disclosed only to persons whose duties reasonably relate to the business purposes for which the information was requested.

**B. Additional Restrictions for BOP and Intelliscore Plus or any other Experian Services containing consumer credit information.** If the Services include either Experian Business Owner Profile Report ("BOP") or Experian Intelliscore Plus Report or any other Experian Services containing consumer credit information, Customer further certifies to Experian and Premium Credit Bureau that it will use the consumer credit information in the BOP and Intelliscore Plus reports or other account monitoring reports solely in connection with a commercial (i.e., not for personal, family or household purposes) credit transaction involving the individual on whom such information is sought, and only if such individual:

(i) is the proprietor of an unincorporated business;

(ii) is a general partner in a partnership;

(iii) is a guarantor of the business' obligation and has provided a copy of a written guaranty; or

(iv) has given written instruction for the provision of such information;

(v) will be used solely as an account monitoring tool when Experian Portfolio Monitoring Services are being provided;

(vi) will be used in compliance with all applicable laws, regulations and ordinances, and all special use restrictions set forth in any agreement with Customer, Premium Credit Bureau and Experian or adopted by Experian or Premium Credit Bureau hereafter; and

(vii) will be maintained in confidence and disclosed only to persons whose duties reasonably relate to the business purposes for which the information was requested.

Every inquiry made on an individual will appear on such individual's Experian Consumer Information Solutions Group consumer credit report, listed as a BOP, SBI or account monitoring inquiry when using these reports, and will include the customer's business name and address.

**C. Warranty Disclaimer and Limitation of Liability.** CUSTOMER FURTHER ACKNOWLEDGES AND AGREES THAT THE DATA AND SERVICES:

(i) ARE PROVIDED ON AN AS IS AND AS AVAILABLE BASIS AND ARE NOT GUARANTEED AND THAT NEITHER THE RESELLER, EXPERIAN NOR THEIR SOURCES WILL BE LIABLE TO THE CUSTOMER FOR ANY LOSS OR DAMAGE BASED ON THE CONTENT OF THE DATA OR SERVICES OR ANY ERRORS OR OMISSIONS THEREFROM;

(ii) ARE SUBJECT TO THE FOLLOWING EXCLUSION OF WARRANTY. RESELLER, EXPERIAN AND THEIR SOURCES DO NOT GUARANTEE OR WARRANT THE ACCURACY, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE SERVICES, DATA OR THE MEDIA ON WHICH THE DATA IS PROVIDED AND SHALL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY RESELLER'S, EXPERIAN'S OR THEIR SOURCES' ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE DATA OR SERVICES. IN NO EVENT SHALL RESELLER, EXPERIAN OR THEIR SOURCES BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS OR LOST PROFITS), WHETHER FORESEEABLE OR NOT, AND HOWEVER CAUSED, EVEN IF RESELLER, EXPERIAN OR THEIR SOURCES ARE ADVISED OF THE POSSIBILITY

OF SUCH DAMAGES. THIS PARAGRAPH STATES RESELLER'S, EXPERIAN'S AND THEIR SOURCES' ENTIRE LIABILITY AND THE SOLE REMEDY OF CUSTOMER IN CONNECTION WITH THE PROVISION OF THE DATA AND SERVICES.

(iii) IF, NOTWITHSTANDING THE PRIOR PARAGRAPH, LIABILITY CAN BE IMPOSED ON RESELLER, EXPERIAN OR THEIR SOURCES, THEN CUSTOMER AGREES THAT THE AGGREGATE LIABILITY FOR ANY OR ALL LOSSES OR INJURIES TO CUSTOMER CONNECTION WITH ANYTHING TO BE DONE OR FURNISHED UNDER THE AGREEMENT, REGARDLESS OF THE CAUSE OR THE LOSS OR INJURY (INCLUDING NEGLIGENCE) AND REGARDLESS OF THE NATURE OF THE LEGAL OR EQUITABLE RIGHT CLAIMED TO HAVE BEEN VIOLATED, SHALL NEVER EXCEED THE AMOUNT PAID TO PREMIUM CREDIT BUREAU FOR THE AFFECTED SERVICES AND CUSTOMER COVENANTS AND PROMISES THAT IT WILL NOT SUE RESELLER, EXPERIAN OR THEIR SOURCES FOR AN AMOUNT GREATER THAN SUCH SUM AND THAT IT WILL NOT SEEK PUNITIVE DAMAGES IN ANY SUIT AGAINST RESELLER, EXPERIAN OR THEIR SOURCES.

## Acknowledgment of Service Agreement

I have read and understand the below:

- ☐ *Payment/Billing Method*
- ☐ *PCB Service Agreement*
- ☐ *Personal Guarantee*
- ☐ *Score Addendum*
- ☐ *Rapid Risk Score Review Service Agreement Addendum*
- ☐ *Multi Bureau Agreement Addendum*
- ☐ *Addendum for OFAC Advisor*
- ☐ *Addendum to Agreement for Internet Service*
- ☐ *Users for Internet Delivery*
- ☐ *Multi Bureau Agreement Addendum - Appendix A*
- ☐ *Access Security Requirements –Appendix B- updated 2014*
- ☐ *GLB Product Addendum-Appendix*
- ☐ *Death Master File Addendum-Appendix D- Updated 2014*
- ☐ *Business credit report Addendum-Appendix C- Updated 2014*

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 test

Title

Date Thu Feb 26 2015 20:21:2

*PCB use only* Accepted by:

_____

Signature

_____

Digital Signature

Name

Title

Date Thu Feb 26 2015 20:21:2

# 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 pre-qualifying 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

---