OneCreditSource.com

Application for Service

Fill in every field. If a field does not apply, mark NA. Failure to complete application may delay processing.

Company Information

Business Name: **Is this the company headquarters?**

Other names or dba's:

Business Type: ☐ C Corp. ☐ S Corp. ☐ LLC ☐ Partnership ☐ Proprietorship ☐ Other:

Principal(s)
Name: _____ Title: _____
Name: _____ Title: _____
Name: _____ Title: _____

Federal Tax ID#: **Date Business Established:**

Number of Employees: **Stock Symbol:**

Physical Address: **Years at location?**

City: **State:** **Zip:**

Do you own or lease this address? ☐ Own ☐ Lease **Is this an executive suite?** ☐ Yes ☐ No

Is this address a private residence? ☐ Yes ☐ No (Businesses operating from a private residence can not receive consumer credit information)

Business Phone #: **Fax #:**

Contact Name: **Contact Title:**

Contact Phone #: **E-Mail:**

Does company have a website? ☐ Yes ☐ No **Website Address:**

Products of Interest:
- ☐ Consumer Reports
- ☐ Commercial Reports
- ☐ Tenant Screening
- ☐ Employment Screening
- ☐ Criminal or Civil Court Records
- ☐ Driving Records
- ☐ Identity Product

Interested in Credit Bureau Access to:
- ☐ TransUnion
- ☐ Equifax
- ☐ Experian

Expected monthly usage:

Billing Information

Billing Address:

City: **State:** **Zip:**

Billing Contact: **Title:** **Phone #:**

Trade References

Business Name: **Account #:**

City: **State:** **Zip:**

Contact: **Title:** **Phone #:**

Business Name: **Account #:**

City: **State:** **Zip:**

Contact: **Title:** **Phone #:**

Signature Required

I certify that the above information is accurate. By signing, I warrant that I have authority to sign on behalf of the company.

Owner, Officer or Authorized Manager (Print): _____ **Title:** _____

→ **Signature:** _____ **Date:** _____

Non-Disclosure & Subscriber Service Agreement

OneCreditsource.com LLC., hereinafter (OCS) is an authorized reseller of, Consumer Reports as defined in the "FCRA".

1. The undersigned ("Subscriber"), desiring to obtain Consumer Reports as defined by the Federal Fair Credit Reporting Act, 15 U.S.C. 1681 et. Seq. ("FRCA") from OCS, agrees that all information, whether oral or written, whether by report, bulletin or otherwise, will be submitted and received subject to the following conditions:

2. Subscriber (Company) _____is a_____*(example: corporation, LLC, etc.)*

   and the nature of its business is _____*(what does your business do?)*

   We will use reports for: _____

   _____

3. Subscriber will request Consumer Reports only when Subscriber intends to use the Consumer Report information (a) in accordance with the FCRA and all state law counterparts; and (b) for the following permissible purposes and no other.

   Reports will be requested in connection with a:
   C Consumer transaction
   B Business transaction (Consumer Credit requests on a business owner require a signed personal guarantee)

   C indicates a Consumer transaction (personal account), **B** indicates a Business transaction (business account). **Check all, which apply:**

   Reports will be used in connection with a transaction involving the consumer or business on whom the information is to be furnished and involving;

C	B	
☐	☐	Extension of credit *
☐	☐	Review of an account *
☐	☐	Tenant Screening *
☐	☐	Due diligence requirements * i.e. potential business partner, government required check
☐	☐	Other legitimate business need in connection with a business transaction that is initiated by the consumer *
		Please explain:_____
☐	☐	Collection of an in house account (We are not a third party collection agency)
☐	☐	Collection of an account by a third party collection agency (We are a third party collection agency)
☐		Employment purposes ***(Subscriber is not authorized to request or receive Consumer Reports for employment purposes unless Subscriber has completed the "Consumer Report for Employment Purpose Addendum" to this Agreement and has been approved by OCS)**

   ***A signed application with appropriate consumer report disclosure is required for all requests**

   Subscriber certifies that it will request consumer reports only for the permissible purpose (s) certified above, and will use the reports obtained for no other purpose.

4. Subscriber certifies it will receive written authorization from the consumer for all permissible purpose categories listed above, with the exception of the collection of an account of the consumer, prior to requesting any consumer report. Subscriber will maintain copies of all written authorizations for a minimum of five (5) years from the date of the inquiry.

5. Subscriber certifies it will make required notifications to consumer for any adverse action taken based on a consumer report. For a copy visit: www.onecreditsource.com/pdf/adverse_action_requirements.pdf
   ☐ **Yes** Subscriber, please check box **AND** initial here _____

6. Subscriber certifies it will make required notifications to any consumer who indicates they are a victim of identity theft. For a copy visit: www.onecreditsource.com/pdf/id_theft_victim_statement_of_rights.pdf
   ☐ **Yes** Subscriber, please check box **AND** initial here _____

7. Subscriber certifies it will assist consumer to dispute errors contained in their consumer report by providing them a copy of a dispute form and directing them to OCS.

8. Subscriber certifies it will have procedures in place to properly dispose of records containing consumer information. Disposal must insure destruction of all identifiable consumer information.

9. Subscriber certifies Consumer Reports will be requested only for Subscriber's exclusive use and solely for the Subscriber's one-time use. Subscriber shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone , in conjunction with subscriber's own data, or otherwise in any service which is derived from consumer reports. Only Subscriber's designated representatives will request Consumer Reports and information will be disclosed only to those employees of Subscriber whose duties reasonably related to their use. Subscriber's employees are forbidden to attempt to obtain reports on themselves, associates or any other persons except in the exercise of their official duties. Subscriber will not disclose the contents of a Consumer Report to the subject of the report except as permitted or required by law.

10. Subscriber shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided , however the subscriber may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, Subscriber shall not disclose to the consumer or any third party, any and all scores provided under this agreement, unless required by law.

11. Subscriber will limit access to Consumer Reports to authorized users only. An authorized user means a Subscriber's employee who has been authorized to request Consumer Reports and has been fully trained on Subscriber's obligations under this Agreement with respect to the ordering and use of Consumer Reports.

12. Subscriber will insure that all devices used to access Consumer Reports are placed in a secure location and accessible only to authorized employees and that these devices are secured when not in use through such means as; screen locks, shutting of power controls, or other commercially reasonable security procedures

13. Subscriber will obtain from OCS a unique user name and password for every authorized user, these will be used solely by that user, and any sharing of information will require the issuing of new user names and passwords. Subscriber will notify OCS immediately of the termination or voluntary separation of any authorized user or of the sharing of any user name or password, to facilitate access termination or password changes. Passwords will change at least every 90 days for all authorized users.

14. Subscriber will monitor compliance with obligations of this Agreement and will notify OCS, immediately upon discovery or detection of any security breach, unauthorized access or attempted unauthorized access to consumer information. Warranty disclaimer: All use of information is at your own risk. You understand and agree the OCS, and its website, services, information, and data are being provided "as-is" without warranty of any kind, whether express or implied, and that they may be subject to delay, deletion, theft, errors or omissions. To the maximum extent permitted by law, OCS, disclaims all warranties, including without limitation, any implied warranties of merchantability, and fitness for a particular purpose, accuracy, and non-infringement.

15. **LIMITATION OF LIABILITY: TO THE MAXIMUM EXTENT PERMITTED BY LAW, OCS, IS NOT RESPONSIBLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROPERTY, LOSS OF DATA, LOSS OF PROFITS, COMPROMISED OR IMPAIRED CLAIMS, LOST SAVINGS, LOST FEES, OR ANY OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATING IN ANY WAY TO THE USE OF PUBLIC RECORDS DATA AND/OR CONSUMER REPORTS RECEIVED FROM OCS, WHETHER BASED ON ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT, NEGLIGENCE OR OTHER TORTS. IN NO EVENT WILL OCS,'S TOTAL LIABILITY TO SUBSCRIBER EXCEED THE FEE PAID BY SUBSCRIBER FOR THE SERVICES PROVIDED OUT OF WHICH THE CLAIM AROSE.**

16. Indemnity: Subscriber shall indemnify, defend, and hold harmless, OCS, its officers, directors, employees, agents, vendors, successors and assigns, from and against all claims, liabilities, suits, actions, losses, damages, costs, expenses, and attorney fees, arising from or related to any claim by Subscriber, the individual(s) to which the Consumer Report pertains, Equifax, Experian, Transunion, and their affiliated companies (collectively "Credit Agencies"), against OCS, pertaining to the publication, disclosure or other use of a Consumer Report supplied to Subscriber by OCS or to any breach by Subscriber of its obligations under this Agreement,. Except as provided below, Subscriber's indemnity obligation hereunder, extends to all claims, counter claims, cross claims, or otherwise, brought or threatened against OCS, by any of the Credit Agencies and/or the individual(s) to which the Consumer Report pertains, arising out of or related to a Consumer Report or any other information provided by OCS, to Subscriber. This section will not apply if the claim, liability or suit arose solely out of the gross negligence or intentional misconduct of an officer of OCS.

17. The laws of the State of Oregon (without giving effect to its conflicts of law principles) govern all matters arising out of or relating to these terms of use, including, without limitation, its validity, interpretation, construction, performance, and enforcement. Any claim, action, suit or proceeding (collectively, "Proceeding" between you and OCS, shall be brought and conducted solely and exclusively within the Circuit Court of the State of Oregon for Clackamas County; provided, however, if a Proceeding must be brought in a federal forum, then unless otherwise prohibited by law, it shall be brought and conducted solely and exclusively within the United States District Court for the District of Oregon.

18. Subscriber shall pay for all services in full at the then current published price, in a timely manner, in accordance with stated terms and conditions.

19. This Agreement shall remain in force and effect until such time as this Agreement is canceled by either party, in writing, with 30 days' notice (Equifax requires only a 10 day notice) but the obligations and Agreement set forth in paragraphs; 4, 8, 14, 15, 16, 17 and 18 above will survive termination of this agreement.

20. THE FCRA 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, OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.

21. With just cause, such as delinquency or violation of the terms of this contract or legal requirement, or a material change in existing legal requirements that adversely affects the Subscriber Agreement, OCS may, upon its election, discontinue serving the Subscriber and cancel this Agreement immediately.

22. OCS may audit Subscribers compliance with the requirements of this Agreement, upon reasonable notice and during normal business hours. The parties recognize that OCS will suffer irreparable harm, and that monetary damages may be incalculable and/or inadequate in the event that Subscriber retains OCS data in breach of Paragraph 1 of this Agreement, and therefore such breach shall be entitled to remedy by injunctive relief, in additional to any and all other relief which may be available at law or at equity.

23. I have read the **"FCRA Requirements and Notice to Users of Consumer Reports"** and understand the obligations of using consumer reports and will abide by them. For a copy visit: www.onecreditsource.com/pdf/fcra_requirements.pdf
☐ **Yes** Subscriber, please check box **AND** initial here _____

24. I have read the **"OneCreditSource.com LLC Data Source Requirements Agreement"** and understand the obligations of using public records data and will abide by them. For a copy visit: www.onecreditsource.com/pdf/data_source_requirements.pdf
☐ **Yes** Subscriber, please check box **AND** initial here _____
☐ **No** Subscriber does not need access to public records data. i.e. criminal or civil court records

25. California Law Certification - Subscriber will refer to Exhibit 1 in making the following certification and Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act. Subscriber certifies it:

☐ **IS** or ☐ **IS NOT** a "Retail seller" as defined in Section 1802.3 of the California Civil Code **AND**
☐ **DOES** or ☐ **DOES NOT** issue credit to consumers who appear in person on the basis of an application for credit submitted in person within the state of California.

26. Vermont Certification - Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Subscriber certifies that it will order Credit Reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA") relating to Vermont residents only after Subscriber has received consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Subscriber certifies that it has received the attached copy of Section 2480e of the VFCR statue. Exhibit 2

I understand and agree to all requirements stated above as conditions for use of any services received from OneCreditSource.com LLC. or its vendors,

Subscriber (Company) Name: _____

Signature: _____

Print: _____

Title: _____

Date: _____

Address: _____

_____

Email: _____

For OneCreditSource.com LLC Use Only

Signature: _____

Print: _____

Title: _____

Date: _____

Consumer Report For Employment Purpose Addendum

1. Subscriber certifies that it will not request a Consumer Report for Employment Purposes unless:
    a. A clear and conspicuous disclosure is first made in writing to the consumer before the report is obtained, in a document that consists solely of the disclosure that a consumer report may be obtained for employment purposes;
    b. The consumer has authorized in writing the procurement of the report; and
    c. Information from the Consumer Report for Employment Purposes will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

2. To comply with section 604 and 609 of the FCRA, subscriber further certifies that before taking adverse action in whole or in part based on the Consumer Report for Employment Purposes, it will provide the consumer:
    a. A complete copy of the Consumer Report for Employment Purposes; and
    b. Copy of the consumer's rights, in the format approved by the FTC, which notice shall be supplied to Subscriber by OCS on all reports.

3. Subscriber agrees that it shall use Consumer Report for Employment Purposes for a one-time use only, and to hold the report in strict confidence, and not to disclose it to any third parties not involved in the current employment decision.

4. The parties hereto agree that this instrument is the full and complete Agreement between them regarding the furnishing of Consumer Report for Employment Purposes, and is not to be altered, varied, or enlarged upon by any verbal promises, statement, or representations not expressed herein. This Agreement shall not be binding on either party until accepted by OCS

Subscriber (Company) Name: _____

Signature: _____

Print: _____

Title: _____

Date: _____

For OneCreditSource.com LLC Use Only

Signature: _____

Print: _____

Title: _____

Date: _____

Exhibit 1

California Retail Seller Requirements

In compliance with California Civil Code and Credit Bureau requirements, OneCreditSource.com LLC requires completion of the following.

Please read the following, check the appropriate box and proceed as directed.

Section 1785.14(a) of the California Civil Code requires all "Retail Sellers" as define in Section 1802.3 (see below) to certify compliance with the requirements stated below.

1802.3. *"Retail seller" or "seller" means a person engaged in the business of selling goods or furnishing services to retail buyers.*

Please sign, date and return this form.

→

☐ NO Subscriber certifies it **IS NOT** a retail seller as defined in Section 1802.3 of the California Civil Code.

☐ YES Subscriber certifies it **IS** a retail seller as defined in Section 1802.3 of the California Civil Code and will abide by the following requirements.

Please read the following carefully. Then sign, date and return this form.

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

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

Section 1785.14(a) (3) If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed.

Subscriber: _____ (Company)

By: _____ (Authorized signer)

Title: _____

Date: _____

Exhibit 2

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

§ 2480e. Consumer consent

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

1. the report is obtained in response to the order of a court having jurisdiction to issue such an order; or
2. the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer.

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

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

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

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

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

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

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

TransUnion: Compliance Requirements

In addition to required OneCreditSource.com documents, all businesses wishing to gain access to TransUnion reports must complete the following and submit all required documentation. These requirements are set forth by TransUnion and must be completed in their entirety before access will be granted to TransUnion reports.

Subscriber (Company Name including all DBA's):_____

Physical Address: _____

Nature of Business: _____

**** Please place a check mark in the appropriate boxes indicating the documents being provided ****

Business License: Check one and provide documents as requested

☐ *Subscriber operates in a geographic location or industry subject to licensing requirements* - subscriber must submit a copy of a current business license reflecting subscriber name and address, which matches subscriber's Application for Service.

☐ *No business license required* (Please provide one of the following **Business License Alternatives**)

Business License Alternatives:

Provide one of the following:

☐ Copy of Federal Tax ID Number ☐ Copy of Articles of Incorporation or Partnership

Business Banking Verification:

☐ We must verify subscriber bank accounts unless subscriber can provide one of the listed alternatives. Please fill out the following and complete the attached **Release Form**.

Bank Name: _____ Account #: _____

Address: _____ City: _____ State: ____ Zip: _____

Contact Person: _____ Title: _____ Phone Number: (____)_____ext_____

Business Banking and Credit Verification Alternative:

As an alternative to business banking and credit verification subscriber may provide one of the following.

☐ A listing with a reputable industry listing or rating, such as A.M. Best's, Moody's, Standard and Poor's, FDIC or NCUA.

☐ A copy of your Annual Report published within the last twelve (12) months and certified by a certified public accounting firm.

New Businesses:

Any business, which has been in business for one (1) year or less, must provide two of the following:

☐ A copy of a utility or telephone bill in the subscriber's name for service at the principal place of business

☐ A copy of lease or proof of property ownership by subscriber of the principal place of business

☐ A copy of a bank statement addressed to the subscriber at its principal place of business

Letter of Intent: (a template of this letter is attached and is also available for download)

☐ On **COMPANY LETTERHEAD** subscriber must indicate; the nature of subscriber's business, subscriber's intended use of TransUnion reports, subscriber's anticipated monthly volume, whether subscriber's access will be primarily local, regional or national. This letter of intent must be signed by; an officer, owner or authorized manager of the subscriber.

Use of Credit Scores:

☐ Subscriber does not intend on using credit scores provided by TransUnion ☐ Subscriber intends on using credit scores provided by TransUnion

Subscriber will request Scores only for Subscriber's exclusive use. Subscriber may store Scores solely for Subscriber's own use in furtherance of Subscriber's original purpose for obtaining the Scores. Subscriber shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except (i) to those employees of Subscriber with a need to know and in the course of their employment; (ii) to those third party processing agents of Subscriber who have executed an agreement that limits the use of the Scores by the third party
to the use permitted to the Subscriber and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii)when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; as required by law.

Subscriber (Company Name): _____ Officer, Owner or Authorized Manager (Print):_____

Signature: **Date:**

Unauthorized Business Types:
TransUnion limits the categories of businesses, which it will provide Consumer Reports. TransUnion will not allow Consumer Reports to be provided to businesses in any of the following categories.

- Adult entertainment service of any kind
- Attorney or Law Firm engaged in the practice of law, unless engaged in collection or using the report in connection with a consumer bankruptcy pursuant to the written authorization of the consumer
- Bail Bondsman, unless licensed by the state in which they are operating
- Credit counseling, except not-for-profit credit counselors
- Credit repair clinic
- Dating service
- Financial counseling, except a registered securities broker dealer
- Genealogical or heir research firm
- Massage service
- Company that locates missing children
- Pawn shop
- Private detective, detective agency or investigative company
- Company that handles third party repossession
- Subscriptions (magazines, book clubs, record clubs, etc.)
- Tattoo service
- Company seeking information in connection with time shares (exception: financiers of time shares)
- Law enforcement agencies
- Asset location services
- News agency or journalist
- Other reseller

Notwithstanding the foregoing these businesses may receive Consumer Reports for Employment Purposes; Law enforcement agencies, detective agencies, law firms, security services, investigators, and lawyers or attorneys at law.

Signature Required

I certify that I understand and will comply with the listed requirements and restrictions for receiving TransUnion reports. I further certify that all information and documents provided are accurate and current. By signing, I warrant that I have authority to sign on behalf of the company (Subscriber).

Subscriber (Company Name) _____

Officer, Owner or Authorized Manager (Print): _____ Title: _____

Signature: _____ Date: _____

The following is required of all Sole Proprietors or Partnerships

Sole Proprietor or Partnership:

If subscriber is a Sole Proprietor or Partnership, the owner or one of the partners must provide the required identification and complete the following consent form:

☐ A copy of government issued photo identification listing the same name, address and date of birth listed on the following;

Consent to obtain a copy of your personal credit report:

Principal's Name: _____Social Security Number: _____ Title: _____

Principal's Current Home Address: _____ Date of Birth: _____

I authorize OneCreditSource.com to request a copy of my personal credit file in order to comply with the requirements to obtain access to "Consumer Credit Reports" from TransUnion.

Signature: Date:

Please:

******COPY THE FOLLOWING LETTER, PASTE ON YOUR COMPANY LETTERHEAD, INSERT YOUR COMPANY NAME & NATURE OF YOUR BUSINESS, FILL OUT AND FAX BACK TO US*******

TransUnion Letter of Intent

YOUR COMPANY NAME is formally requesting approval from Trans Union and OneCreditSource.com to gain the ability to pull consumer credit reports, social security number trace's &/or employment consumer credit reports.

The nature of our business is: **NATURE OF YOUR BUSINESS**

We intend to use these reports in the following manner (check all that apply):
_____ Extension of Credit
_____ Collection of our Own Accounts
_____ Collections (We are a 3rd party debt collection agency)
_____ Employment Screening
_____ Tenant Screening
_____ Other (please explain) _____

We anticipate on pulling _____ reports per month.

We anticipate our access to be primarily:
_____ LOCAL
_____ REGIONAL
_____ NATIONAL

YOUR COMPANY NAME conforms to very high standards of integrity and quality, and we will abide by all current and future regulations and compliance changes that OneCreditSource.com and the National Credit Bureaus set forth.

We, **YOUR COMPANY NAME,**

_____ **DO** intend to use credit scores provide by TransUnion.
_____ **DO NOT** intend to use credit scores provide by TransUnion.

End User will request Scores only for End User's exclusive use. End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining the Scores. End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except (i) to those employees of End User with a need to know and in the course of their employment; (ii) to those third party processing agents of End User who have executed an agreement that limits the use of the Scores by the third party to the use permitted to the End User and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii)when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; as required by law.

End User (Company Name): _____

Officer, Owner or Authorized Manager Signature: _____

Print: _____

Date: _____

OneCreditSource.com

Release Form

The Subscriber is attempting to establish an account with OneCreditSource.com, a subsidiary of Background Investigations. As part of the qualification process, Background Investigations will need to obtain the information below on the company's bank account and trade references. By signing below, the Subscriber hereby authorizes this information to be released to a representative of Background Investigations. The Subscriber is a duly authorized representative of the company.

Subscriber /Company Name: _____

Authorized Signature _____ Authorized Signature _____

Printed Name _____ Printed Name _____

Date _____ Date _____

For Official Office Use Only – Subscriber Not To Write In This Box

Bank/Trade Name: _____

Account #: _____

Date Account Opened: _____ Average Balance: _____

Verified by: _____ Type of Account: _____

Date: _____

Trade

Date Account Opened: _____ Rating: _____

Current Balance: _____ High Credit: _____ Terms: _____

Manner Of Payment: _____ Current Status: _____

Verified by: _____ Date: _____

Please return the completed form to:

Compliance Manager
Fax: (800) 905-9736
Phone: (800) 905-9678
Attn: Compliance Manager

Equifax: Compliance Requirements

In addition to required OneCreditSource.com documents, all businesses wishing to gain access to Equifax reports must complete the following and submit all required documentation. These requirements are set forth by Equifax and must be completed in their entirety before access will be granted to Equifax reports.

Subscriber (Company Name including all DBA's):_____

Business Address: _____

Nature of Business: _____

**** Please place a check mark in the appropriate boxes indicating the documents being provided ****

Business License: Check one and provide documents as requested

☐ *Subscriber operates in a geographic location or industry subject to licensing requirements* - subscriber must submit a copy of a current business license reflecting business name and address, which matches subscriber's Application for Service.

☐ *No business license required* (please provided one of the following **Business License Alternatives**)

Business License Alternatives:

☐ Copy of Articles of Incorporation or Partnership
☐ Copy of professional license issued by the state
☐ Proof of regulation under the FCRA section 621 (b) (1,2 or3)
☐ Copy of State Tax ID Certification
☐ Proof of 5019 (c) (3) status
☐ Copy of Federal Tax ID Number

Copy of lease or proof of ownership: REQUIRED (unless company is publicly traded)

☐ A copy of the pages of your lease that contain: signature, address and terms of your lease
☐ Proof of ownership (i.e. property tax statement)

Use of Credit Scores:

☐ I do not intend on using credit scores provided by Equifax
☐ I intend on using credit scores provided by Equifax (Complete the Equifax Credit Score Use Agreement)

Unauthorized Business Types:

Equifax limits the categories of businesses, which it will provide Consumer Reports. Equifax will not allow Consumer Reports to be provided to businesses in any of the following categories.

- Adult entertainment service of any kind
- Business that operates out of an unrestricted location within a residence
- Attorney or Law Firms (except collection attorneys, bankruptcy attorneys, or those attorneys who use reports solely for employment purposes)
- Bail Bondsman
- Check cashing
- Credit counseling
- Credit repair clinic or any type of company involved in credit repair activity
- Dating service
- Financial counseling (except housing counseling agencies)
- Genealogical or heir research firm
- Massage service
- Company that locates missing children
- Pawn shop
- Private detective, detective agency or investigative company
- Individuals seeking information for their private use (including individual landlords)
- Company that handles third party repossession
- Company of individual involved in spiritual counseling
- Subscriptions (magazines, book clubs, record clubs, etc.)
- Tattoo service
- Insurance Claims

Signature Required

I certify that I understand and will comply with the listed requirements and restrictions for receiving Equifax reports. I further certify that all information and documents provided are accurate and current. By signing, I warrant that I have authority to sign on behalf of the company (Subscriber).

Subscriber (Company Name) _____

Officer, Owner or Authorized Manager (Print): _____ Title: _____

Signature: _____ Date: _____

The following is required of Corporations in business for less than one year and all Sole Proprietors or Partnerships

Corporations in business for less than one year or any Sole Proprietorship or Partnership:
(Not required for publicly traded companies)

If business is a Corporation in business for less than one year or any Sole Proprietorship or Partnership, a personal credit report is required on the owner, one of the partners or an officer of the corporation.

The owner, one of the partners or an officer of the corporation must provide the required documents and complete the following:
☐ A copy of government issued photo identification listing the same name, address and date of birth listed on the following;

Consent to obtain a copy of your personal credit report:

Principal's Name: _____Social Security Number: _____ Title: _____

Principal's Current Home Address: _____ Date of Birth: _____

I authorize OneCreditSource.com to request a copy of my personal credit file in order to comply with the requirements to obtain access to "Consumer Credit Reports" from Equifax.

Signature: **Date:**

Equifax: Beacon Score Use Agreement

1. Subscriber, desiring to use EQUIFAX's BEACON, agrees that all BEACON services and information, whether oral or written, whether by report or otherwise, will receive subject to the following conditions:

2. The BEACON service consists of point-scorable prediction algorithms developed by The Fair Isaac Companies ("**Fair, Isaac**"). It is based on the computerized consumer credit information in EQUIFAX's automated consumer credit reporting systems, and design to predict the risk of an individual not paying accounts as agreed. EQUIFAX will apply BEACON to those Subscriber inquiries for consumer reports from EQUIFAX's automated consumer credit reporting systems as Subscriber may request. Pursuant to such an inquiry and request for BEACON information, EQUIFAX will, as available, provide Subscriber the BEACON score, up to four of the principal factors contributing to the BEACON score, and the consumer credit report.

3. BEACON information from EQUIFAX will be requested only for the exclusive use of the Subscriber, and all BEACON information received from EQUIFAX will be held in strict confidence by Subscriber, except to the extent that disclosure to others is permitted or required by law.

4. Subscriber will hold EQUIFAX, Fair, Isaac and all their credit agents and employees harmless on account of any expense or damage arising or resulting from the publishing or other disclosure by Subscriber or Subscriber's employees or agents, of the BEACON score, the credit report or other information contrary to the conditions set forth in **Paragraph 3**.

5. Subscriber understands that requests for use of the Beacon for Account Management and/or Prescreening programs are not authorized under this Agreement.

6. Subscriber will comply with the provisions of the Federal Fair Credit Reporting Act, 15 U.S.C. Section 1681 et. seq., as amended (the "**FCRA"**), the Equal Credit Opportunity Act, 15 U.S.C. Section 1681 et. seq., as amended (the "**ECOA"**), all state law counterparts of them, and all applicable regulations promulgated under any of them, including without limitation, any provision requiring adverse action notification to the consumer. Equifax will comply with the provisions of the Federal Fair Credit Reporting Act, 15 U.S.C. Section 1681 et. seq., as amended (the "**FCRA"**), all state law counterparts of it, and all applicable regulations promulgated under it.

7. EQUIFAX does not guarantee the predictive value of the BEACON scores with respect to any of Subscriber's applicants or customers, and does not intend to characterize any such individual as to credit capability and the BEACON score only represents and estimate of credit risk relative to other individuals in EQUIFAX's automated consumer reporting system and any predictive value only represents an opinion based on the point scorable prediction algorithms. Subscriber releases EQUIFAX, Fair, Isaac, their officers, employees, agents, sister or affiliated companies, or any third party contractors or suppliers of EQUIFAX from liability for any damages, losses, costs, or expenses, whether direct or indirect, suffered or incurred by Subscriber resulting from the use of BEACON or any failure of BEACON to accurately predict the creditworthiness of Subscriber's applicants and customers in connection with Subscriber's actions in regard to it's applicants and customers. In the event BEACON was not correctly applied by EQUIFAX to the credit file, the **Subscriber's** sole remedy and EQUIFAX's sole responsibility will be to reprocess the credit file through BEACON at no additional charge. SUBCRIBER AGREES THAT FAIR, ISAAC, ECIS, THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SISTER OR AFFILIATED COMPANIES OR ANY THIRD PARTY CONTRACTORS OR SUPPLIERS ARE NOT RESPOSIBLE FOR ANY LOSS OF PROFITS, SPECIAL, INDIRECT, CONSEQUESTIONAL OR EXEMPLARY DAMAGES, COSTS OR EXPENSES IN CONNECTION WITH THE USE OR PERFORMANCE OF BEACON SCORES EVEN IF ADVISED OF THE POSSIBILITES OF SUCH DAMAGES. The combined liability of Equifax and Fair, Isaac arising from BEACON scores provided by EQUIFAX and Fair, Isaac shall be limited to the aggregate amount of money received by EQUIFAX from Subscriber from the use of BEACON under this Agreement during the preceding twelve (12) months prior to the date of the event that gave rise to the cause of action.

8. EQUIFAX has received a warranty from Fair, Isaac, the developer of BEACON, stating that the scoring algorithms used in the computation of the BEACON score are empirically derived from EQUIFAX's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to credit risk, and no scoring algorithm(s) used by BEACON uses a "prohibited basis" as that term is defined in the ECOA and Regulation B, and promulgated thereunder and EQUIFAX reasonably believes such warranty is true.

9. EQUIFAX is the authorized agent of Fair, Isaac for purposes of executing this Agreement as it pertains to the BEACON score and for collection of all fees and charges arising thereunder with respect to the BEACON scores.

10. Subscriber will hold all BEACON scores received from EQUIFAX under this Agreement in strict confidence and will not disclose any BEACON score to the consumer except as required by law. Subscriber may provide the principal factors

contributing to the BEACON scores to the subject of the report when those principal factors are the basis of Subscriber's adverse action against the subject consumer. Subscriber must describe the principal factors in a manner which complies with Regulation B, of the ECOA. Further, Subscriber acknowledges that the BEACON scores and factors are proprietary and that, except for (a) disclosure to the subject consumer if Subscriber has taken adverse action against such consumer based in whole or in part on the consumer report with which the BEACON scores to any other party without EQUIFAX's and Fair, Isaac's prior written consent.

11. Subscriber warrants that, before delivering or directing EQUIFAX to deliver BEACON scores to any third party, Subscriber will enter into a contract with such third party that (a) limits the use of the BEACON scores by the third party only to the use permitted to Subscriber and (b) identifies EQUIFAX and Fair, Isaac as express third party beneficiaries to such contract.

12. Subscriber shall not use BEACON scores as the basis for an "Adverse Action" as defined by the Equal Credit Opportunity Act or Regulation B, unless score factor codes have been delivered to Subscriber along with the BEACON score.

13. All BEACON services will be charged to Subscriber at the regular rates of EQUIFAX in the city in which the service is rendered, and Subscriber will apy charges upon rendition of monthly or yearly statements.

14. Subscriber understands that the BEACON score and principal reasons are only one of various items of information it can use in connection with it's review and decision regarding the subject. Subscriber certifies that BEACON information will only be requested along with a consumer report, and that a consumer report, as defined by the FCRA, will be ordered only when intended to be used for "permissible purposes" as defined by the FCRA. Subscriber is not authorized to request or receive BEACON for employment purposes under this agreement.

15. This Agreement is supplemental to the Agreement for Service for consumer credit reporting services entered into between Subscriber and EQUIFAX, which is incorporated herein by reference. This Agreement applies just to information furnished by EQUIFAX to Subscriber from the BEACON System and sets forth the entire understanding and agreement between EQUIFAX and Subscriber regarding on-line BEACON services.

16. Written notice by any party will terminate this Agreement, but the obligations and agreements set forth in **Sections 3, 4, 5, 6, 7, 10** and **17** will remain in force.

17. This Agreement may be modified only by a written amendment duly executed by all parties. No party may assign its rights or obligations except with prior written consent of the other parties. This Agreement shall be interpreted in accordance with the internal laws (and not the conflicts of laws) of the State of Georgia. The undersigned is a duly authorized representative with all powers required to execute this Agreement.

18. Authority. Equifax's delivery of the services Client orders under this Agreement indicates Equifax's acceptance of the Agreement. The person signing below represents and warrants that he or she has the necessary authority to bind the principal (s) set forth below.

IN WITNESS WHEREOF, the undersigned has executed this Agreement as of the date written below.

Subscriber (Company Name): _____

Address: _____

_____

Signature: _____

Print Name: _____

Title: _____

Date: _____

Experian: Compliance Requirements

In addition to required OneCreditSource.com documents, all businesses wishing to gain access to Experian reports must complete the following and submit all required documentation. These requirements are set forth by Experian and must be completed in their entirety before access will be granted to Experian reports.

Subscriber (Company Name including all DBA's): _____

Physical Address: _____

Nature of Business: _____

**** Please place a check mark in the appropriate boxes indicating the documents being provided ****

Business License:

☐ If business is required to have an industry specific license (i.e. mortgage license) subscriber must submit a copy of a current license reflecting business name and address, which matches your Application for Service.

☐ No industry specific license required (please provide one of the following **Business License Alternatives**)

Business License alternatives:

Provide one of the following:

☐ Copy of current Business License
☐ Copy of Federal Tax ID Number
☐ FDIC Certificate
☐ Copy of Articles of Incorporation or Partnership
☐ Copy of State Tax ID Certification
☐ Documentation of ticker symbol information from trading website

Business License alternatives for Publicly Traded Companies:

Provide one of the following:

☐ Certified copy of audited annual or quarterly statement submitted to the Securities Exchange Commission
☐ Documentation of ticker symbol information from trading website

---

☐ **Access Security Requirements** (the Access Security Requirements Agreement is attached and signed)**:**

In order to protect the privacy and information of consumers, certain security measures must be in place. This agreement explains your responsibilities and must be signed by: an officer, owner or authorized manager of the subscriber.

Use of credit Scores:

☐ I do not intend on using credit scores provided by Experian
☐ I intend on using credit scores provided by Experian (Complete the Experian Credit Score Use Agreement)

Tenant Screening:

Provide one of the following:

☐ 3 signed rental applications (either new of existing tenants)
☐ Documents from Landlord/Tenant Court with proof of filing
☐ Verified membership in local/regional/national Apartment Association

SELECT YOUR BUSINESS TYPE AND PROVIDE THE REQUIRED DOCUMENTS

☐ **Property management company**
  ☐ A signed list of all properties under management

☐ **Individual landlord**

Provide **one** of the following for ***each*** rental property
  ☐ Copy of filed property title
  ☐ Property insurance documents from county/city/state
  ☐ Copy of filed property tax records

Provide the following for ***each*** rental property
  ☐ A signed rental application or agreement

Provide the following for identification
  ☐ State or Federal Photo ID

☐ **Independent Real Estate agent** contracted with a real estate firm for tenant screening purposes
  ☐ Copy of Real Estate Brokers license
  ☐ Documented verification of the business relationship from the real estate firm (Documentation must include: name of institution, name of person providing verification, phone number of institution, verification of business name)

Unauthorized Business Types:
Experian limits the categories of businesses, which it will provide Consumer Reports. Experian will not allow Consumer Reports to be provided to businesses in any of the following categories.

- Bail bond companies
- Internet locator services
- Diet centers
- Adoption search firms
- Investigative companies (i.e., private investigators and private detective agencies), except those licensed for – and exclusively practicing, investigative work for employment purposes and noted is
- Attorneys and paralegal firms (other than attorneys whose sole and exclusive practice is collections)
- Law enforcement agencies (except for employment purposes)
- Dating services
- Asset location services (does not include collection agencies or with respect to GLB products)
- Future services, such as health clubs, timeshares, continuity clubs, etc. (except health clubs (spas) human resource departments for employment purposes) without written approval from Experian
- Media, news agencies or journalists
- Businesses which operate out of a residence
- Credit clinics; credit repair organizations
- Credit counseling services without prior approval from Experian
- Any company (or individuals) who is known to have been involved in credit fraud or other unethical business practices
- Organizations or companies on Experian customer Alert List
- Companies involved and/or associated with inappropriate adult content web sites and/or adult-type telephone services

Signature Required

I certify that I understand and will comply with the listed requirements and restrictions for receiving Experian reports. I further certify that all information and documents provided are accurate and current. By signing, I warrant that I have authority to sign on behalf of the company (Subscriber).

Subscriber (Company Name) _____

Officer, Owner or authorized manager (Print): _____ Title: _____

Signature: _____ Date: _____

Experian: Score Use Agreement

This Credit Scoring Services Agreement, ("Agreement"),

Dated: _____Between _____("End User")
Company Name

_____

Company Street Address City State ZIP Telephone

and OneCreditSource.com ("reseller") and Experian Information Solutions, Inc., acting through its Information Solutions Division and Fair, Isaac and Company, Incorporated (collectively "Experian/Fair, Isaac").

For good and valuable consideration and intending to be legally bound, End User and Reseller and Experian/Fair, Isaac hereby agree as follows:
Terms of Resale Contracts. All contracts between Reseller and End Users for the resale of the Scores and reason codes generated by the Experian/Fair, Isaac Model shall contain the following provisions, each of which is material.

I. The End User's warranty that it has a "permissible purpose" under the Fair Credit Reporting Act, as it may be amended from time to time, to obtain the information derived from the Experian/Fair, Isaac Model.

II. The End User's agreement to limit its use of the Scores and reason codes solely to use in its own business with no right to transfer or otherwise sell, license, sublicense or distribute said Scores or reason codes to third parties;

III. 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;

IV. Notwithstanding any contrary provision of the End User Agreement, End User may disclose the Scores provided to End User under this End User Agreement to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only.

V. A requirement that each End User comply with all applicable laws and regulations in using the Scores and reason codes purchased from Reseller;

VI. A prohibition on the use by End User, its employees, agents or subcontractors, of the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of Experian Information Solutions, Inc. or Fair, Isaac and Company, or the affiliates of either of them, or of any other party involved in the provision of the Experian/Fair, Isaac Model without such entity's prior written consent;

VII. A prohibition on any attempts by End User, in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian/Fair, Isaac in performing the Experian/Fair, Isaac Model;

VIII. WARRANTY. Experian/Fair, Isaac warrants that the Experian/Fair, Isaac Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Experian/Fair Model is applied is similar to the population sample on which the Experian/Fair, Isaac Model was developed, the Experian/Fair, Isaac Model score may be relied upon by Reseller and/or End Users to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to End Users. Experian/ Fair, Isaac further warrants that so long as it provides the Experian/Fair Isaac 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 EXPERIAN/FAIR, ISAAC HAVE GIVEN RESELLER AND/OR END USERS WITH RESPECT TO THE EXPERIAN/FAIR, ISAAC MODEL AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EXPERIAN/FAIR, ISAAC MIGHT HAVE GIVEN RESELLER AND/OR END USERS WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANT ABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Reseller and each respective End User's right under the foregoing Warrant are expressly conditioned upon each respective End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.).

IX. A provision limiting the aggregate liability of Experian/Fair, Isaac to each End User to the lesser of the Fees paid by Reseller to Experian/Fair, Isaac pursuant to consideration of Experian/Fair, Isaac's performance of the Experian/Fair, Isaac Model, Reseller will pay Experian/Fair, Isaac fees (the "Fees") as agreed upon in writing by Reseller and Experian/Fair, Isaac from time to time. Pursuant to this, 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 Reseller 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.

Complete Agreement. This agreement sets forth the entire understanding of End User, Reseller and Experian/Fair, Isaac with respect of the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.
IN WITNESS WHEREOF, the undersigned has executed this agreement as of the date written below:

Subscriber (Company Name): _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

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

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

1. Implement Strong Access Control Measures

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

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

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

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

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

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

1.7 Develop strong passwords that are:

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Maintain a Vulnerability Management Program

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

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

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

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.

- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. <u>Protect Data</u>

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. <u>Maintain an Information Security Policy</u>

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 Experian within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with

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

5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access Experian systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

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

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

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

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

7. Mobile and Cloud Technology

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

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

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

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

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

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

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

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

8. **General**

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

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

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

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

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

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

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 Experian systems shall be made available to Experian upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Experian 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 Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian 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 800-295-4305, Email notification will be sent to regulatorycompliance@experian.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 Experian 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 Experian networking and computing resources may be monitored and audited by Experian, 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 Experian 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 Experian.

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

General requirements:

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

Roles and Responsibilities

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

2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

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

_____ _____

Signature Date

_____ _____

Print Name/Title (authorized signer on account) Company Name

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.
Subscriber Code	Your seven digit Experian account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided

	within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Experian Customer Certificate: Commercial Credit Addendum

This Customer Certificate is executed as of the date set forth below by the undersigned customer (hereinafter referred to as "Customer") for the benefit of OneCreditSource.com (hereinafter referred to as "Reseller") and Experian Information Solutions, Inc., acting through its Business Information Solutions Group (hereinafter referred to as "Experian").

A. Restrictions on Use. In consideration for Customer's right to receive and use certain data and services (collectively, the "Services") from Reseller and Experian, Customer understands and certifies to Experian and Reseller 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 Reseller 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 SBI, or any other Experian Services containing consumer credit information. If the Services include either Experian Business Owner Profile Report ("BOP") or Experian Small Business Intelliscore ("SBI") Report or any other Experian Services containing consumer credit information, Customer further certifies to Experian and Reseller that it will use the consumer credit information in the BOP and SBI 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, Reseller and Experian or adopted by Experian or Reseller 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 not guaranteed and that neither the Reseller, Experian nor their sources will be liable to the Customer for any loss or damage based on any errors or omissions there from;

(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 RESELLER 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.

Name of Customer: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____