

Please read these terms and conditions of use carefully before accepting them by clicking the “I AGREE” button.

**UNIVERSAL MEMBERSHIP AGREEMENT
for
Equifax Verification Services**

Use of this website and the Equifax Verification Services (provided by TALX Corporation) (“EVS”) is expressly conditioned upon acceptance of the terms and conditions set forth in this Agreement (“Agreement”). By accepting these terms and conditions, User agrees to be legally bound by them and intends this to be an agreement accepted and signed by User. If User does not agree with any part of the following terms and conditions, User must promptly either exit this website or click “I Decline,” and User may not use this website or the services offered herein. User may exit this website at any time.

RECITALS:

A. EVS operates The Work Number®, a service used to verify employment and income information about individuals (“Consumers”), and various other services used to verify certain Consumer information (EVS’ services are collectively referred to herein as the “Service”); and

B. Company wishes to use the Service to verify certain Consumer information.

C. For the purposes of this agreement, “Company” refers to any user, and/or any company User represents, accessing this website or using the Service through the use of the username and password that have been, or may be, assigned pursuant to acceptance of these terms and conditions.

NOW, THEREFORE, the parties agree as follows:

1. SCOPE OF THE AGREEMENT. This Agreement consists of the general terms set forth in the body of this Agreement, Exhibit 1, Exhibit 2, Exhibit 3, and each Schedule A executed by the parties which may contain additional terms. If there is a conflict between the general terms and conditions of this Agreement and any Exhibit or Schedule, the provisions of the Exhibit or Schedule will govern and control. This Agreement specifically supersedes and replaces any agreement between the parties that predates this Agreement and which relates to the Service as provided in each Schedule A, even if the prior agreement contains an “entire agreement” or “merger” clause, and any such agreements are terminated.

2. EVS OBLIGATIONS. The Service will provide Company with automated access to certain employment and/or income data (“Data”) furnished to EVS by employers.

3. COMPANY OBLIGATIONS.

a. Company shall comply with the terms set forth in this Agreement which includes Exhibits 1, 2, and 3, and also Schedule A, which may contain additional terms.

b. Company shall pay for the Services in the manner and amount communicated to Company. All prices are exclusive of, and Company shall pay, all sales, use, privilege, or excise taxes.

c. Company certifies that it will order Data from the Service only when Company intends to use the Data (i) in accordance with the Fair Credit Reporting Act (“FCRA”) and all state law FCRA counterparts as though the Data is a consumer report, and (ii) for one of the following FCRA permissible purposes: (1) in connection with a credit transaction involving the Consumer on whom the Data is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer, (2) in connection with the underwriting of insurance involving the Consumer, (3) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with an existing credit obligation, (4) when Company otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the Consumer, or to review an account to determine whether the Consumer continues to meet the terms of the account; or (5) for employment purposes and for no other purpose. Company agrees to only use the Data consistent with the obligations of users of consumer reports as provided for in the Consumer Financial Protection Bureau (the “CFPB”)’s Notice Form attached as Exhibit 1. Company certifies that before ordering Data to be used in connection with employment purposes, it will clearly and conspicuously disclose to the subject Consumer, in a written document consisting solely of the disclosure, that Company may obtain Data for employment purposes and will also

obtain the Consumer's written authorization to obtain or procure Data relating to that Consumer. Company further certifies that it will not take adverse action against the consumer based in whole or in part upon the Data without first providing to the Consumer to whom the Data relates a copy of the Data and a written description of the Consumer's rights as prescribed by the CFPB, and also will not use any Data in violation of any applicable federal or state equal opportunity law or regulation. Company acknowledges that it has received from EVS a copy of the consumer rights summary as prescribed by the CFPB as referenced on Exhibit 3.

d. Company certifies that it will comply with applicable provisions under Vermont law. In particular, Company certifies that it will order Data relating to Vermont residents only after Company has received prior Consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Company further certifies that the attached copy of VFCRA Section 2480e applicable Vermont Rules as referenced in Exhibit 2 was received from EVS.

e. Company may use the Data provided through the Service only as described in this Agreement. Company may reproduce or store the Data obtained from the Service solely for its own use in accordance with this Agreement, and will hold all Data obtained from the Service under this Agreement in strict confidence and will not reproduce, reveal, or make it accessible in whole or in part, in any manner whatsoever, to any others unless required by law, or unless Company first obtains EVS's written consent; provided, however, that Company may discuss Consumer Data with the Data subject when Company has taken adverse action against the subject based on the Data. Company will not provide a copy of the Data to the Consumer, except as may be required or permitted by law or approved in writing by EVS, except in any state where this contractual prohibition would be invalid. Company will refer the Consumer to EVS whenever the Consumer disputes the Data disclosed by Company. Company will not interpret the failure of EVS to return Data as a statement regarding that consumer's credit worthiness, because the failure may result from one or more factors unrelated to credit worthiness.

f. Company will comply with the provisions of the FCRA, the Federal Equal Credit Opportunity Act, as amended (the "ECOA"), all state law counterparts of them, and all applicable regulations promulgated under any of them, including, without limitation, any provisions requiring adverse action notification to the Consumer.

g. Company acknowledges it shall employ decision-making processes appropriate to the nature of the transaction and in accordance with industry standards and will use the Data as part of its processes.

h. Company may access, use and store the Data only at or from locations within the territorial boundaries of the United States, Canada, and the United States territories of Puerto Rico, Guam and the Virgin Islands (the "Permitted Territory"). Company may not access, use or store the Data or EVS Confidential Information at or from, or send the Data or Confidential Information to, any location outside of the Permitted Territory without Company first obtaining EVS' written permission.

i. Company may not allow a third party service provider (hereafter "Service Provider") to access, use, or store the Service or Data on its behalf without first obtaining EVS's written permission.

j. In order to ensure compliance with this Agreement, applicable law and EVS policies, EVS may conduct reviews of Company activities, from time to time, during normal business hours, at all locations containing relevant records, with respect to Company's requests for Data and/or its use of Data. Company shall provide documentation within a reasonable time to EVS as reasonably requested for purposes of such review. Company (i) shall cooperate fully with any and all investigations by EVS of allegations of abuse or misuse of the Services and allow EVS to access its premises, records, and personnel for purposes of such investigations if EVS deems such access is necessary to complete such investigation(s), (ii) agrees that any failure to cooperate fully and promptly in the conduct of any audit constitutes grounds for immediate suspension of the Service and/or termination of the Agreement, and (iii) shall promptly correct any discrepancy revealed by such investigation(s).

4. DATA SECURITY. This Section 4 applies to any means through which Company orders or accesses the Service including, without limitation, system-to-system, personal computer or the Internet. For the purposes of this Section 4, the term "Authorized User" means a Company employee that Company has authorized to order or access the Service and who is trained on Company's obligations under this Agreement with respect to the ordering and use of the Service, and the Data provided through same, including Company's FCRA and other obligations with respect to the access and use of Data.

a. Company will, with respect to handling any Data provided through the Service:

1. Ensure that only Authorized Users can order or have access to the Service,

2. Ensure that Authorized Users do not order Data for personal reasons or provide Data to any third party except as permitted by this Agreement,
3. Inform Authorized Users that unauthorized access to Data may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment,
4. Ensure that all devices used by Company to order or access the Service are placed in a secure location and are accessible only by Authorized Users, and that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures,
5. Take all necessary measures to prevent unauthorized ordering of or access to the Service by any person other than an Authorized User for permissible purposes, including, without limitation, (i) limiting the knowledge of the Company security codes, user names, User IDs, and any passwords Company may use, to those individuals with a need to know. In addition, the User IDs must be unique to each person, and the sharing of User IDs or passwords is prohibited,
6. Change Company's user passwords at least every ninety (90) days, or sooner if an Authorized User is no longer responsible for accessing the Service, or if Company suspects an unauthorized person has learned the password. . Additionally, perform at least quarterly entitlement reviews to recertify and validate Authorized User's access privileges,
7. Adhere to all security features in the software and hardware Company uses to order or access the Services, including the use of IP restriction,
8. Implement secure authentication practices when providing User ID and passwords to Authorized Users, including but not limited to using individually assigned email addresses and not shared email accounts,
9. In no event access the Services via any unsecured wireless hand-held communication device, including but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals and portable data terminals
10. Not use non-company owned assets such as personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, and DVDs) to store the Data. In addition, Data must be encrypted when not in use and all printed Data must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose. In either case, commercially reasonable practices for the type of Data received from EVS must be employed,
11. If Company sends, transfers or ships any Data, encrypt the Data using the following minimum standards, which standards may be modified from time to time by EVS: Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms,
12. Not ship hardware or software between Company's locations or to third parties without deleting all EVS Company number(s), security codes, User IDs, passwords, Company user passwords, and any consumer information, or Data,
13. Monitor compliance with the obligations of this Section 4, and immediately notify EVS if Company suspects or knows of any unauthorized access or attempt to access the Service, including, without limitation, a review of EVS invoices for the purpose of detecting any unauthorized activity.
14. If, subject to the terms of this Agreement, Company uses a Service Provider to establish access to the Service, be responsible for the Service Provider's use of Company's user names, security access codes, or passwords, and Company will ensure the Service Provider safeguards Company's security access code(s), User IDs, and passwords through the use of security requirements that are no less stringent than those applicable to Company under this Section 4,
15. Use commercially reasonable efforts to assure data security when disposing of any Data obtained from EVS. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Company's activities (e.g. the Federal Trade Commission, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records,

16. Use commercially reasonable efforts to secure Data when stored on servers, subject to the following requirements: (i) servers storing Data must be separated from the Internet or other public networks by firewalls which are managed and configured to meet industry accepted best practices, (ii) protect Data through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iii) secure access (both physical and network) to systems storing Data, which must include authentication and passwords that are changed at least every ninety (90) days; and (iv) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available,

17. Not allow Data to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices,

18. Use commercially reasonable efforts to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history for at least three (3) months for review,

19. Provide immediate notification to EVS of any change in address or office location and are subject to an onsite visit of the new location by EVS or its designated representative, and

20. In the event Company has a security incident involving EVS Confidential Information, Company will fully cooperate with EVS in a security assessment process and promptly remediate any finding.

b.If EVS reasonably believes that Company has violated this Section 4, EVS may, in addition to any other remedy authorized by this Agreement, with reasonable advance written notice to Company and at EVS's sole expense, conduct, or have a third party conduct on its behalf, an audit of Company's network security systems, facilities, practices and procedures to the extent EVS reasonably deems necessary, including an on-site inspection, to evaluate Company's compliance with the data security requirements of this Section 4.

5. CONFIDENTIALITY. Each party acknowledges that all materials and information disclosed by a party ("Disclosing Party") to another party ("Recipient") in connection with performance of this Agreement, including Data, the terms of this Agreement and the pricing terms contained in Schedule A, consist of confidential and proprietary data ("Confidential Information"). Each Recipient will hold those materials and that information in strict confidence, and will restrict its use of those materials and that information to the purposes anticipated in this Agreement. If the law or legal process requires Recipient to disclose confidential and proprietary data, Recipient will notify the Disclosing Party of the request. Thereafter, the Disclosing Party may seek a protective order or waive the confidentiality requirements of this Agreement, provided that Recipient may only disclose the minimum amount of information necessary to comply with the requirement. Recipient will not be obligated to hold confidential any information from the Disclosing Party which (a) is or becomes publicly known, (b) is received from any person or entity who, to the best of Recipient's knowledge, has no duty of confidentiality to the Disclosing Party, (c) was already known to Recipient prior to the disclosure, and that knowledge was evidenced in writing prior to the date of the other party's disclosure, or (d) is developed by the Recipient without using any of the Disclosing Party's information. The rights and obligations of this Section 5 (i) with respect to confidential and proprietary data that constitutes a "trade secret" (as defined by applicable law), will survive termination of this Agreement for so long as such confidential and proprietary information remains a trade secret under applicable law; and (ii) with respect to all other confidential and proprietary data, will survive the termination of this Agreement for the longer of two (2) years from termination, or the confidentiality period required by applicable law.

6. RIGHTS TO SERVICE. The Service and the Data are proprietary to EVS and all rights to the Service and Data are proprietary to and reserved by EVS.

7. WARRANTY. EVS warrants that the Service will be performed in all material respects in a reasonable and workmanlike manner and in compliance with laws and regulations applicable to EVS's performance thereof. Company acknowledges that the ability of EVS to provide accurate information is dependent upon receipt of accurate information from employers. EVS does not warrant that the Service will be error free. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH HEREIN, EVS MAKES NO OTHER WARRANTIES AS TO THE SERVICE OR THE DATA, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF GOOD TITLE, MERCHANTABILITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE EVEN IF EVS KNOWS OF SUCH PURPOSE.

8. TERM AND TERMINATION. This Agreement shall be for an annual term, and shall be automatically renewed for successive one year terms. Either EVS or Company may terminate this Agreement or any Schedule(s), at any time upon ten (10) days prior written notice to the other. If EVS believes that Company has breached an obligation under

this Agreement, EVS may, at its option and reserving all other rights and remedies, terminate this Agreement and/or any Schedules immediately upon notice to Company.

9. MODIFICATION. Notwithstanding Section 13 below, EVS may change the price of the Service and/or the Service Description by updating the pricing, Service Description, and/or terms and conditions on the web interface for ordering verifications, which Company shall acknowledge and agree to in order to continue receiving the Service through EVS.

10. INDEMNIFICATION AND LIMITATION OF LIABILITY. Company and EVS recognize that every business decision represents an assumption of risk and that neither party in furnishing Confidential Information, Data, or the Service to the other, underwrites or assumes the other's risk in any manner. Each party agrees to indemnify, defend and hold harmless ("Indemnify") the other party and its affiliates, and their directors, officers and employees (each, an "Indemnified Party"), from and against claims, demands, liabilities, suits, damages, expenses and costs, including reasonable attorneys', experts' and investigators' fees and expenses ("Claims") brought by third parties against the Indemnified Party and arising from the indemnifying party's, or its affiliates', directors', officers' or employees' ("Indemnifying Party") (i) breach of this Agreement, (ii) negligent or intentional, wrongful act or omission, (iii) infringement on third party proprietary rights, (iv) violation of law, or (v) breach of Section 5 Confidentiality.

In no event shall EVS or its officers, agents or employees be liable for loss of profits or for indirect, special, incidental or consequential damages arising out of or related to the Service or this Agreement, even if it has been advised of the possibility of such damages. Except for the indemnification obligations found herein, damages of any kind payable by EVS shall not exceed the sum paid by Company for the item of Service which causes Company's claim.

11. APPLICABLE LAW. This Agreement shall be governed by the laws of the State of Missouri, without giving effect to the principles of conflict of laws thereof.

12. FORCE MAJEURE. Neither party will be liable to the other for any delay, or interruption in performance as to any obligation hereunder resulting from governmental emergency orders, judicial or governmental action, emergency regulations, sabotage, riots, vandalism, labor strikes or disputes, acts of God, fires, electrical failure, major computer hardware or software failures, equipment delivery delays, acts of third parties, or delays or interruptions in performance beyond its reasonable control.

13. MISCELLANEOUS. This Agreement sets forth the entire agreement between the parties regarding the Service. Except as otherwise provided in this Agreement, this Agreement may be amended only by a subsequent writing signed by both parties. This Agreement may not be assigned or transferred by Company without EVS's prior written consent. This Agreement shall be freely assignable by EVS and shall inure to the benefit of and be binding upon the permitted assignee of either Company or EVS. If any provision of this Agreement is held to be invalid or unenforceable under applicable law in any jurisdiction, the validity or enforceability of the remaining provisions thereof shall be unaffected as to such jurisdiction and such holding shall not affect the validity or enforceability of such provision in any other jurisdiction. To the extent that any provision of this Agreement is held to be invalid or unenforceable because it is overbroad, that provision shall not be void but rather shall be limited only to the extent required by applicable law and enforced as so limited. Any notice under this Agreement shall be effective upon delivery by an overnight or other courier or delivery service, or three (3) days after pre-paid deposit with the postal service, in either case to the party's address in the first sentence of this Agreement or any substitute therefore provided by notice, or by email to the email address on record with EVS.

Company acknowledges receipt of Exhibit 1, "Notice to Users of Consumer Reports, Obligations of Users". Furthermore, Company has read "Notice to Users of Consumer Reports, Obligations of Users" which explains Company's obligations under the FCRA as a user of consumer report information (To be initialed by the person signing on behalf of Company).

By clicking "I AGREE," User certifies that (i) User is authorized to execute this Agreement on behalf of User and any person or user that User represents, (ii) TALX Corporation (provider of Equifax Verification Services) has reasonable grounds to assume and deem it apparent that User has such authority, (iii) this Agreement is a binding obligation of User and any person or company that User represents, (iv) User has carefully reviewed to user's complete satisfaction and understands and agrees to all of the terms and conditions above and accessible below by scrolling down, and intend this to be a binding agreement signed by User accepting and agreeing to all such terms and conditions. User may print these terms and conditions. TALX Corporation (provider of Equifax Verification Services) recommends that User print these terms and conditions, and save them for User's files.

**UNIVERSAL MEMBERSHIP AGREEMENT
for
The Work Number® Verifier Services**

Exhibit 1

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

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

The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the CFPB's website.

Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.

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

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

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

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

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

3. Adverse Actions Based on Information Obtained From Affiliates

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

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

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

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

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

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

A. Employment Other Than in the Trucking Industry

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

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

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

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by

an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in federal regulations) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF “PRESCREENED” LISTS

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

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.

- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
 1. the identity of all end-users;
 2. certifications from all users of each purpose for which reports will be used; and
 3. certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

The CFPB's website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

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

Section 602 15 U.S.C. 1681
 Section 603 15 U.S.C. 1681a
 Section 604 15 U.S.C. 1681b
 Section 605 15 U.S.C. 1681c
 Section 605A 15 U.S.C. 1681cA
 Section 605B 15 U.S.C. 1681cB
 Section 606 15 U.S.C. 1681d
 Section 607 15 U.S.C. 1681e
 Section 608 15 U.S.C. 1681f
 Section 609 15 U.S.C. 1681g
 Section 610 15 U.S.C. 1681h
 Section 611 15 U.S.C. 1681i
 Section 612 15 U.S.C. 1681j

Section 613 15 U.S.C. 1681k
Section 614 15 U.S.C. 1681l
Section 615 15 U.S.C. 1681m
Section 616 15 U.S.C. 1681n
Section 617 15 U.S.C. 1681o
Section 618 15 U.S.C. 1681p
Section 619 15 U.S.C. 1681q
Section 620 15 U.S.C. 1681r
Section 621 15 U.S.C. 1681s
Section 622 15 U.S.C. 1681s-1
Section 623 15 U.S.C. 1681s-2
Section 624 15 U.S.C. 1681t
Section 625 15 U.S.C. 1681u
Section 626 15 U.S.C. 1681v
Section 627 15 U.S.C. 1681w
Section 628 15 U.S.C. 1681x
Section 629 15 U.S.C. 1681y

**UNIVERSAL MEMBERSHIP AGREEMENT
for
The Work Number® Verifier Services**

Exhibit 2

VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

The undersigned, _____ (“Company”), acknowledges that it subscribes to receive various information services from TALX Corporation, provider of Equifax Verification Services (“EVS”), in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the “VFCRA”), and the federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. seq., as amended (the “FCRA”), and its other state law counterparts. In connection with Company's continued use of EVS services in relation to Vermont consumers, Company hereby certifies as follows:

Vermont Certification. Company certifies that it will comply with applicable provisions under Vermont law. In particular, Company certifies that it will order Data relating to Vermont residents, that are credit reports as defined by the VFCRA, only after Company has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules. Company further certifies that the attached copy of VFCRA § 2480e applicable Vermont Rules were received from EVS.

Company: _____

Signed By: _____

Printed Name and Title: _____

Account Number: _____

Date: _____

Please also include the following information:

Compliance Officer or Person Responsible for Credit Reporting Compliance

Name: _____

Title: _____

Mailing Address: _____

E-Mail Address: _____

Phone: _____ Fax: _____

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 consumer's credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent.

**UNIVERSAL MEMBERSHIP AGREEMENT
for
The Work Number® Verifier Services**

Exhibit 3

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and

specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. **For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.**

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment - or to take another adverse action against you - must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your “file disclosure”). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.consumerfinance.gov/learnmore for additional information.

- You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.
- You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.consumerfinance.gov/learnmore for an explanation of dispute procedures.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.
- Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.
- Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need - usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.
- You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.consumerfinance.gov/learnmore.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. Unsolicited “prescreened” offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. You may opt out with the nationwide credit bureaus at 1-888-5-OPT OUT (1-888-567-8688).
- You may seek damages from violators. If a consumer reporting agency, or in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.
- Identity theft victims and active duty military personnel have additional rights. For more information, visit www.consumerfinance.gov/learnmore.

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General. For information about your federal rights, contact:

TYPE OF BUSINESS:	CONTACT:
<p>1.a. Banks, savings associations, and credit unions with total assets of over \$10 billion and their affiliates.</p> <p>b. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the CFPB:</p>	<p>a. Consumer Financial Protection Bureau 1700 G Street NW Washington, DC 20552</p> <p>b. Federal Trade Commission: Consumer Response Center - FCRA Washington, DC 20580 (877) 382-4357</p>
<p>2. To the extent not included in item 1 above:</p> <p>a. National banks, federal savings associations, and federal branches and federal agencies of foreign banks</p> <p>b. State member banks, branches and agencies of foreign banks (other than federal branches, federal agencies, and Insured State Branches of Foreign Banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act</p> <p>c. Nonmember Insured Banks, Insured State Branches of Foreign Banks, and insured state savings associations</p> <p>d. Federal Credit Unions</p>	<p>a. Office of the Comptroller of the Currency Customer Assistance Group 1301 McKinney Street, Suite 3450 Houston, TX 77010-9050</p> <p>b. Federal Reserve Consumer Help Center P.O. Box 1200 Minneapolis, MN 55480</p> <p>c. FDIC Consumer Response Center 1100 Walnut Street, Box #11 Kansas City, MO 64106</p> <p>d. National Credit Union Administration Office of Consumer Protection (OCP) Division of Consumer Compliance and Outreach (DCCO) 1775 Duke Street Alexandria, VA 22314</p>
<p>3. Air carriers</p>	<p>Asst. General Counsel for Aviation Enforcement and Proceedings Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, SE Washington, DC 20590</p>
<p>4. Creditors Subject to Surface Transportation Board</p>	<p>Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, SW Washington, DC 20423</p>
<p>5. Creditors Subject to Packers and Stockyards Act, 1921</p>	<p>Nearest Packers and Stockyards Administration area supervisor</p>
<p>6. Small Business Investment Companies</p>	<p>Associate Deputy Administrator for Capital Access United States Small Business Administration 409 Third Street, SW, 8th Floor Washington, DC 20416</p>
<p>7. Brokers and Dealers</p>	<p>Securities and Exchange Commission 100 F Street, NE Washington, DC 20549</p>
<p>8. Federal Land Banks, Federal Land Bank Associations, Federal Intermediate Credit Banks, and Production Credit Associations</p>	<p>Farm Credit Administration 1501 Farm Credit Drive McLean, VA 22102-5090</p>
<p>9. Retailers, Finance Companies, and All Other Creditors Not Listed Above</p>	<p>FTC Regional Office for region in which the creditor operates or Federal Trade Commission: Consumer Response Center - FCRA Washington, DC 20580 (877) 382-4357</p>

UNIVERSAL MEMBERSHIP AGREEMENT
SCHEDULE A – BUSINESS CLASS
SERVICE DESCRIPTION

I) COMPANY USE OF SERVICE:

The Work Number® is an employment verification service provided by TALX Corporation (a provider of Equifax Verification Services), a Missouri corporation (“EVS”), to its employer clients. Data on the Service may be accessed by company to verify Consumer’s employment status (“The Work Number® Employment Verification”) or income (“The Work Number® Income Verification”) for commercial purposes. EVS shall provide the Service in accordance with the Universal Membership Agreement (“Agreement”), Exhibit 1, Exhibit 2 and Exhibit 3 to the Agreement and this Schedule A (which is part of this Agreement). All defined terms used herein shall have the meaning ascribed to them in the Agreement.

a) Business Class Product. The Work Number® Employment Verification includes the Consumer’s (i) employer name, (ii) employer address, (iii) employment status, (iv) most recent hire date, (v) total length of service, and (vi) position title, where available. The Work Number® Income Verification includes Data provided in The Work Number® Employment Verification, plus the most recent two years of payroll Data, where available. The Business Class Service delivers The Work Number® Employment Verification or The Work Number® Income Verification Data available for the requested combination of Consumer and Employer Name or Code.

b) Delivery.

i) **Online.** The Service will provide automated access to requested Data via the internet.

c) Input Requirements.

i) **Online.** Company may obtain The Work Number® Employment Verification by providing a Consumer’s social security number and the employer name, or employer code. Company may obtain The Work Number® Income Verification by providing a Consumer’s social security number, the employer name, or employer code, and a current salary key code.