



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 1

List View

General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 330405

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0511

Vendor ID: VS0000014336 

SO Doc ID: BCF1800000001

Legal Name: Equifax Inc

Published Date: 11/20/17

Alias/DBA:

Close Date: 11/28/17

Total Bid: \$558,000.00

Close Time: 13:30

Response Date: 11/28/2017 

Status: Closed

Response Time: 13:01

Solicitation Description: Employment Verification Services - Addendum #1 

Total of Header Attachments: 1

Total of All Attachments: 1

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|------|----------------------------------|-------------|------------|-------------|-----------------------------|
| 1 | Employment Verification Services | 50000.00000 | EA | \$11.160000 | \$558,000.00 |

| Comm Code | Manufacturer | Specification | Model # |
|-----------|--------------|---------------|---------|
| 83120000 | | | |

| | |
|-------------------------------|--|
| Extended Description : | 3.1.1 Employment Verification Services |
|-------------------------------|--|

WV DHHR Employment Verification Services
Response for RFQ # 0511 BCF1800000001

West Virginia

Department of Health and Human Resources

November 28, 2017



November 28, 2017

April Battle

2019 Washington Street East
Charleston, WV 25305-0130
Email: april.e.battle@wv.gov

Dear Ms. Battle:

TALX Corporation (a provider of Equifax Verification Services) ("Equifax") appreciates the opportunity to respond to the West Virginia Department of Health and Human Resources (DHHR) Request for Quote dated October 13, 2017. Equifax understands the requirements set forth by the State and we believe our solution will uniquely address your needs. Our goal is to deliver a best in class identity proofing solution which will allow the citizens in the State of West Virginia quickly and easily gain access to the services and sites that they need. We believe you will find this RFQ response demonstrates our expertise, commitment and dedication toward helping DHHR quickly stand up and manage an Employment Verification Services.

Equifax's verification platform is currently deployed in 40+ States and several Federal Agencies including Center for Medicare and Medicaid Studies (CMS) as well as the Social Security Administration. Our verification platform is easily configurable and ready for immediate deployment either through our web portal or through a system to system API integration. Equifax has over 100+ years of supplying customers with unique data and insights. In addition to Asset and Property verification, we are also uniquely positioned to deliver Employment and Income data, Identity Verification, Residency and Phone Number verification, Identity authentication and verification, as well as any other State or partner owned data set all through a single API or portal. We look forward to working with the State and exceeding the State expectations when delivering Employment Verification services.

During your evaluation process, I will be your point of contact for questions and clarification. Please contact me via email at kurt.jones@equifax.com or at (314) 214-7080.

Equifax looks forward to establishing very successful, long-term partnership with you. We are confident that Equifax can and will meet all of the business needs and requirements posed by DHHR and hope to have an opportunity to present our solution in person.

Sincerely,

Kurt D. Jones

Account Executive

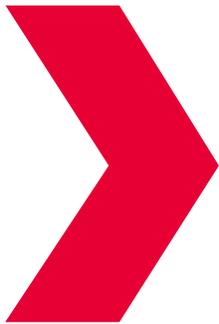
Equifax Government Services

O 314-214-7080

C 314-941-2677

kurt.jones@equifax.com

Disclaimer



No information contained herein may be reproduced or communicated to any third party except as required by law or with the express written consent of TALX Corporation (a provider of Equifax Verification Services) (“Equifax”). Equifax will not be liable for any claims, third party or otherwise, related to the information provided herein.

While provided in good faith, this proposal is intended to be a framework for discussion and is nonbinding. The terms of any final agreement must be reviewed and approved by Equifax prior to execution. Neither the proposal recipient nor Equifax shall be legally bound unless and until the parties execute a definitive written agreement. All information contained in our response will remain effective for 90 days from November 28, 2017.

Contents

| | |
|---|----|
| Disclaimer | ii |
| Executive Summary | 1 |
| Understanding Your Challenges | 1 |
| Recommended Approach..... | 2 |
| Delivering Value | 2 |
| Our Expertise..... | 2 |
| Moving Forward Together | 3 |
| Equifax Eligibility Advisor Overview..... | 4 |
| Pricing | 7 |
| Pricing Terms and Conditions | 8 |
| Attachments | 9 |
| Amendments Acknowledgement..... | 9 |
| Exceptions to Terms and Conditions..... | 10 |
| Universal Membership Agreement for Government Agencies..... | 11 |
| Contact Us | 12 |

Executive Summary

Knowledge = Information

As a global information solutions company, Equifax is committed to providing knowledge that helps its customers make informed decisions. Developing unparalleled analytical insights that leverage our unique data is one of our enduring corporate imperatives. We are conditioned to anticipate our customers' needs and focused on innovating to meet those needs. Our new slogan—Powering the World with Knowledge—sums up our vision and strategy for supporting our customers.

Equifax has proven experience supporting the entire lifecycle of Federal and state benefit programs across the United States. Our solutions are utilized in 43 different states to streamline eligibility determinations, reduce fraud, automate recertification and analyze mission performance of a given program. Typical challenges we've incorporated in our solutions include confirming identity, verifying eligibility and helping stakeholders adhere to their organization's demands. Our Equifax pedigree is built on the *I.D.E.A Framework*:

- **Identity:** We have identity information for more than 820 million people worldwide, and are regularly adding new identity capabilities to prevent improper payments.
- **Data:** We have built a 360-degree view of benefit eligibility, combining identity, asset, income, telecom/utilities, real property, public records and third-party data sources with our credit data using our proprietary keying and linking technologies.
- **Exchanges:** We have a proven track record of building and operating data exchanges on behalf of industry that allow us to validate, verify, and reconcile identities and organizations to detect benefit fraud.
- **Analytics:** We have a robust analytics platform for decisioning and risk management to enable evidence-based decision making.

Having a partner that knows the Public Sector and implements best practices is essential to establishing and maintaining class leading capabilities in fraud, waste and abuse detection.

Understanding Your Challenges

As stated in the RFQ, the West Virginia Department of Health and Human Resources (DHHR) Employment Verification Services (EVS) must provide employment verification for the Bureau for Children and Families. The Employment Verification Services shall:

- Employment Verification Services must provide functionality of employment verification for applicants or recipients that include their present and past employer(s) names, their current employment status, and current income verification.
- The AVS Services must provide employer's name, employer's address, dates of employment, individual's availability of medical and/or dental insurance, present and past pay rate, bonus payments, and at least three (3) years of year-to-date income and pay period details.

Drawing on our experience addressing similar objectives/challenges for other Government organizations customers, we've developed an approach to meet all of your needs today and well into the future.

Recommended Approach

The Equifax solution is implemented leveraging Equifax's **Eligibility Advisor** data services hub, which employs a highly secure web services architecture that utilizes industry-standard RESTful / JSON web services. Eligibility Advisor is the same solution used by Equifax to deliver other social service verification services, including asset, employment and income verifications.

Equifax's solution also includes a complete web-based administrative interface that provides the capability for customer support representatives and analysts to research transactions, generate and deliver a variety of on-demand reports, and includes both service configuration and administrative capabilities – including robust user/group/role-based access controls for the administrative application itself.

Delivering Value

Our Expertise

We strongly believe that building strategic partnerships with our clients enables our clients to effectively use our services, resulting in increased revenue, productivity, and efficiency. Here are just a few reasons why Equifax is clearly the choice for your organizations current and future initiatives:

- **Experience** – Equifax brings to DHHR more than 115 years of experience providing credit risk assessment, fraud detection, and marketing solutions.
- **Your Equifax Client Team** – DHHR will be supported by experienced professionals who know your company and are specialists in the Government services. Every member of our team is ready to work within every level of your organization to visit current opportunities, industry trends, and new products and services; solve problems together; and invigorate the spirit of strategic partnership.
- **Innovation** – Equifax has earned numerous awards in the areas of identity verification, fraud and modeling, employing new technologies our competitors constantly strive to imitate. In 2016, Equifax introduced 53 new products. New Product Innovation (NPI) has proven to be a valuable and centralized discipline for product development and innovation on both a national and global scale at Equifax. While credit bureau activities are a vital part of our business, we have been expanding our expertise for many years in the areas that are vital to your business success.
- **Value** – Price is never the true measure of value, only a component. We believe Equifax offers DHHR the most valuable combination of services, capabilities, and resources available in our industry. Equifax is committed to continuously enhancing its solutions and, as part of that effort, maintains a roadmap for each product and service that outlines specific plans to maintain our position in the market.

Moving Forward Together

Equifax has invested more than \$1.6 billion over the last few years in new technology, data assets, and information solutions that offer an unmatched, multidimensional suite of services to solve customer problems and introduce solutions that our competitors are not offering.

As you conduct your evaluation, please keep in mind what distinguishes our approach from others that you may consider. Our approach delivers:

- “Investment Grade” Verification
- A more efficient and more in depth Verification process
- Regulatory compliance, maintaining compliance controls and audit requirements
- Real time verification
- Access to the most up to date information



Equifax's verification platform is currently deployed in 40+ States and several Federal Agencies including Center for Medicare and Medicaid Studies (CMS) as well as the Social Security Administration.

We trust our proposal clearly reflects our profound interest in your success. At Equifax, you will find a company that is ready, enthusiastic, and deeply committed to your vision as well as your satisfaction. We want to be of service to DHHR for this endeavor.

Equifax Eligibility Advisor Overview

To support the State of West Virginia's functional requirements, and position the agency with a flexible data services HUB, Equifax will configure, integrate and deploy the **Equifax Eligibility Advisor (EA)** product. The EA product is based on our proven enterprise platform that is currently in use in over 100 clients across the private sector, state government, and federal agencies including CMS and the USPS and is deployed in the Commonwealth of Kentucky's verification solution.

The EA product platform is comprised of an application engine for processing of enrollment requests, a rules engine for defining business process workflows; a data services hub for integration of Equifax, partner and client data sources; and a data warehouse for reporting and analysis. EA is deployed under a "hosted and managed service" business model. This delivery model offers the flexibility and customization that would typically accrue from an in-house solution and combines that with the operational, financial, and security benefits associated with a solution fully hosted by the Equifax team.

EA's flexible, service-oriented architecture allows the Equifax team to quickly implement the requirements for an employment verification and identification service configured and deployed to provide an API-based, real-time interface as well as batch services for the delivery of verification data. No matter what medium of delivery, Equifax has experience providing eligibility solutions in Web/Portal, API integration or Batch capabilities. Our EA Platform is configured to support the State's functional requirements & we will deliver employment verification data to support DHHR and another other publically administered benefits programs.

To meet the needs of WVDHHR, as outlined in this RFQ, Equifax will configure and deploy our real-time web portal to be used by WVDHHR's employees and will support a minimum of 1200 and a maximum of 1500 users. The EA web portal will be available to WVDHHR employees during the business hours as defined in the RFQ (Monday-Friday, 7 A.M. – 7 P.M.) and will be completely secure, available via standard web browsers over HTTPS.

Through the different mediums, the EA Platform can be leveraged to support verifications by pulling from proven Equifax and partner data services including:

- **Income and Employment Verifications** – Equifax's The Work Number database, which is currently deployed to and utilized by the State
- **Identity, DOB, and SSN Verifications** – Equifax's proven identity suite of products that are in use by numerous federal and state agencies providing services and benefits to a similar demographic
- **Real Property Asset Verifications (physical assets)** – Equifax's robust asset verification solution provides real time and manual verification of real property assets held by an individual to include, but not limited to: land, homes, mobile homes and vehicles.
- **Financial resource, holdings and/or account verifications** – Equifax's robust solution for financial asset discovery and balance history that derives its data from the same sources other competitors use to perform these services.

Eligibility Advisor accepts any number and combination of data elements such as Name (First and Last), Date of Birth, Social Security Number, Address, State, City and ZIP Code to initiate a

data search. Eligibility Advisor leverages Equifax’s identity resolution capabilities to more accurately identify the correct identity when utilizing a combination of the desired data search attributes. Internally, Equifax follows a master data management approach based on a “person master file,” and each individual identity, residential address and household is identified with a unique key. These keys can also be used as search criteria, or to link and confirm that two records refer to the same person or household (i.e. deduplication of records in a single database or across databases).

As a simple example, a typical two-stage workflow involves a query against Equifax’s identity verification product to first validate the identity of the individual, match against attributes such as name and address, and then query Eligibility Advisor’s asset verification service using the matched identity’s SSN. Since both products are called in real-time, to the end user this workflow appears as a single step with a single entry form, or is available as a single API request/response, or via batch. For a more complex example, the State might define separate workflow orchestrations for each social service program it administers (for example, a “Medicaid ABD” workflow).

The platform’s flexibility allows Equifax to utilize it internally, both as a componentized data hub and as the application framework for several of our identity and fraud products. The underlying application and rules engine that are a part of Eligibility Advisor can be used to integrate and apply business rules across Equifax data products and services, third-party products, services, and customer data – with existing data connectors for over 100 internal and third-party products and the capability to easily define new data source connectors. This provides the State a platform that can later be used to create waterfall strategies that leverage data from the Federally Facilitated Marketplace (FFM) to support states Medicaid and CHIP verifications processing activities, or to seamlessly import State or county-level data, such as DMV or other sources.

Many different pieces of data can be used to describe an individual from credit, utility billing address & history, employment & income, automobile, property and asset information. Should WV and/or DHHR require different verification services, there are additional components native to Equifax which can be leveraged.

Table 1: Eligibility Advisor Capabilities and Benefits Overview

| Data Type | Benefit to West Virginia |
|---|--|
| Proprietary Income and Employment Data | <ul style="list-style-type: none"> • Unique, up-to-date data that is more current and reliable than state wage or National New Hire data • Fewer false negatives/positives produces better decisions • Employers update records an average of 2.7x per month, the most recent data available • Current employer-direct payroll data is industry standard, tens of millions records available • Current and historical employment and income provide accurate view of applicant’s wages • Collection of 157 fields of employment and income data • Employment data beyond that of initial new hire date • Gross and Net Income provided by employers, both may be used for eligibility decisions • Full-year income history that may include bonus, salary increases, hours worked, leaves of absence, and other |

| | |
|-----------------------------|---|
| | <p>valued data</p> <ul style="list-style-type: none"> • Benefits data as provided by some employers • Ability to monitor past verifications and detect status changes |
| Property data | <ul style="list-style-type: none"> • 100 million historical property records from county deeds • 90% of the records drawn from assessor and recorder files • 40 million multiple-listing service (MLS) records, providing best-in-class data coverage and accuracy • Understand actual property values and look back historically on the following pieces: <ul style="list-style-type: none"> • Assessed Property Data: Property characteristics (beds, baths, sq. footage, etc.), geographic location (latitude/longitude for parcel boundary records), and FIPS location codes • Ownership and Lien Data: Identity of the property owner(s), Origination amounts, dates, lien types, title and escrow information • Assessed and Automated Values: Both annual assessed values and Equifax AVM can be returned, providing one of the most reliable, current property valuation models on the market |
| Financial asset data | <ul style="list-style-type: none"> • Asset search and return in real time based on records checks provides instant results • Data contributed directly by financial institutions to a trusted industry consortium, the largest available |

Equifax’s track record is one of implementing complex projects on-time. Our Government Services organization would work directly on the requirements as outlined in this RFQ to ensure fulfillment. We are responsive, deeply committed, experienced and have access to many benefits/exchange Subject Matter Experts (SMEs) on the team. We are excited about this opportunity and the chance to further grow our relationship.

Pricing

Table 2: Exhibit A - Pricing Page

| Line Item | Description | Estimated Quantity | Cost | Extended Cost |
|-----------|--|--------------------|---------|---------------|
| 3.1.1 | Verification of employment hits per year | 50,000 | \$11.16 | \$558,000.00 |
| | | | Total | \$558,000.00 |

**Equifax has provided pricing as specified in Exhibit A – Pricing. Additional cost savings can be realized via alternate pricing models (e.g. commitment of a specific volume) and will be open to review estimated usage.*

| |
|---|
| VENDOR NAME: TALX Corporation (a provider of Equifax Verification Services) |
| ADDRESS: 11432 Lackland Road, St. Louis, MO 63146 |
| FAX #: 314-214-7588 |
| PHONE #: 314-214-7000 |
| E-MAIL ADDRESS: ian.hilton@equifax.com |
| REMIT TO ADDRESS: 4076 Paysphere Circle, Chicago, IL60674 |
| SIGNATURE:  Ian Hilton, Director Government Services |
| DATE: November 28, 2017 |

Pricing Terms and Conditions

- Rates are based on a contract term of 1 year, which shall commence on the first day of the billing month following execution of a formal Agreement.
- Upon expiration of the Agreement, EVS will suspend service until a new Agreement is in place.
- Rates are based on product description, data elements, and use-case as described. Any change to these statements or descriptions requires approval by both parties and may result in rate modification.
- A hit is defined by a database search which successfully returns data. The above pricing is based on one use/decision per hit.
- Notwithstanding anything herein or the Agreement to the contrary, in the event Agency terminates this Agreement prior to the end of the current term, Agency shall pay one hundred percent (100%) of the remaining Annual Amount due and overages if applicable.

Attachments

Amendments Acknowledgement

TALX Corporation acknowledges receiving of Addendum # 1 dated 11/20/2017. A signed copy of the Addendum provided below.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ 0511 BCF180000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

TALX Corporation
Company

Ellen Stanke
Authorized Signature

11/27/17
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

SOLICITATION NUMBER: CRFQ 0511 BCF1800000001
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as (“Solicitation”) to reflect the change(s) identified and described below.

Applicable Addendum Category:

- Modify bid opening date and time
- Modify specifications of product or service being sought
- Attachment of vendor questions and responses
- Attachment of pre-bid sign-in sheet
- Correction of error
- Other

Description of Modification to Solicitation:

To provide the vendor questions and responses.

No other changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM #1 TO RESPOND TO VENDOR QUESTIONS

Vendor Question #1

The solution called for by this RFP may involve the provision of “consumer reports” (as that term is defined and used in the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. Section 1681) to Agency. Accordingly, and notwithstanding anything to the contrary in this RFP, if, in its response to this RFP, Contractor proposes to provide consumer reports to Agency, Contractor may also include with its proposal additional contract terms and conditions related to: (a) Contractor’s obligations and the nature of its operations as a “consumer reporting agency” under the FCRA and related laws, rules, and policies; and (b) Agency’s obligations and the nature of its operations as a “user” of consumer reports under the FCRA and related laws, rules, and policies. Subject to Agency review and negotiation, such additional terms and conditions may be included in a final contract if awarded to the contractor that proposed them.

Is the State willing to review alternate terms and conditions and additional terms as noted above due to FCRA and related laws, rules and policies?

Agency Response to Vendor Question #1

Any alternate or additional terms and conditions must be submitted with the bid package to be considered by the Agency. Acceptance in whole or in part will be at the State’s discretion.

Vendor Question #2

Please confirm that forms “Disclosure of Interested Parties to Contracts”, “PURCHASING AFFIDAVIT” and “VENDOR PREFERENCE CERTIFICATE” are not required to be submitted with the proposal package on December 1, 2017, and could be provided later before the Award.

Agency Response to Vendor Question #2

The Disclosure of Interested Parties and Purchasing Affidavit should be included with the vendor’s bid, however, they can be provided later before the award.

The Vendor Preference Certificate must be completed and submitted with the vendor’s bid if the vendor is claiming Vendor Preference. If the vendor is not claiming Vendor Preference the form is not required.

Vendor Question #3

Section 3.1 (Qualifications): Must have an employment database containing a minimum of 4500 employers. Can you please provide more information regarding the above statement? Is the database about SEcurecheck360’s internal database of having 4500 clients?

Agency Response to Vendor Question #3

Yes, the employment database that the verification results will be based on, must contain data from a minimum of 4500 employers.

Vendor Question #4

Section 4.1.1.4 (Mandatory Requirements): Must update employment database with current information at least once daily.

Can you please elaborate more on the above statement?

Agency Response to Vendor Question #4

The employment database must be updated with current information at least once daily. As an employment verification request takes place, the information results must be derived from data that is current by being updated at least once daily.

Exceptions to Terms and Conditions

The Fair Credit Reporting Act (“FCRA”) governs the collection, assembly, and use of consumer report information. As a federally regulated consumer reporting agency, Equifax must comply with the FCRA and related laws, rules, and policies. Users of consumer reports, including state agencies verifying employment status or income to determine eligibility for state administered programs, also have various obligations under the FCRA. Failure to comply with the FCRA can result in administrative, civil, and even criminal repercussions.

In order to meet the requirements of the FCRA, Equifax has developed a “Universal Membership Agreement” (“UMA”) for government agencies that wish to use the verification services Equifax offers, a copy of which is attached. The UMA contains terms and conditions unique to the nature of Equifax’s highly regulated consumer reporting services, most of which are designed to ensure Equifax exercises its “grave responsibilities with fairness, impartiality, [] a respect for the consumer’s right to privacy, [and] in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of” the FCRA. These terms and conditions include, for example:

- Certification by the government agency that the consumer report data will only be used for a statutorily-enumerated “permissible purpose” (see FCRA §§ 604 and 607);
- Agreement by the government agency to provide notice to consumers under various circumstances described throughout the FCRA (see, e.g., FCRA § 615);
- Measures to ensure Equifax is able to provide mandatory disclosures and notifications to consumers whose information has been accessed by the agency (see FCRA § 609);
- Language contemplating the proprietary nature of the data and services Equifax provides;
- Appropriate disclaimers given the nature of the data and services Equifax provides;
- Data security requirements to protect consumer privacy; and
- Certifications by the government agency necessary to comply with other relevant federal and state laws (e.g., Vermont-specific requirements).

Equifax currently provides verification services to government agencies in almost all states and to multiple federal agencies, each of which has necessarily incorporated into their contracts terms and conditions consistent with those described, above. Equifax respectfully proposes incorporation of its UMA into the contract should Equifax’s proposal be selected for contract award. One way this could be expeditiously accomplished is by incorporating the UMA by reference along with an order of precedence clause stating the UMA takes precedence; if the agency would like to revise certain terms of the UMA, Equifax would be happy to discuss those specific terms with the agency prior to finalizing the contract.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Kurt Jones
(Name, Title)
Account Executive
(Printed Name and Title)
11432 Lackland Rd St. Louis MO 63146
(Address)
(314) 214-7080
(Phone Number) / (Fax Number)
kurt.jones @ equifax.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

TALX Corporation
(Company)
Ellen Stanko
(Authorized Signature) (Representative Name, Title)
Ellen Stanko, VP Solutions
(Printed Name and Title of Authorized Representative)
11/27/2017
(Date)
(314) 214-7000
(Phone Number) (Fax Number)

Universal Membership Agreement for Government Agencies

UNIVERSAL MEMBERSHIP AGREEMENT
for
The Work Number[®] for Government Agencies

This **Universal Membership Agreement** (the “Agreement”) is entered into by and between TALX Corporation (a provider of Equifax Verification Services), a Missouri Corporation, located at 11432 Lackland Road, St. Louis, Missouri (“EVS”), and _____ located at _____ (“Agency”), and is effective as of this 11.1.2017 (the “Effective Date”).

RECITALS:

- A. EVS operates The Work Number[®], a service used to verify employment and income information about an individual (“Consumers”), and various other services used to verify certain Consumer information (EVS’s services are collectively referred to herein as the “Service”); and
- B. Agency wishes to use the Service to verify certain Consumer information.

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, including any Exhibits and Schedules attached hereto. 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 related to a Service that predates this Agreement, even if the prior agreement contains an “entire agreement” or “merger” clause, and any such agreements are hereby terminated.
- 2. EVS OBLIGATIONS.** The Service will provide Agency with automated access to certain employment and/or income data (“Data”) furnished to EVS by its employer clients.
- 3. AGENCY OBLIGATIONS.**
 - a. Agency shall comply with the terms set forth in this Agreement.
 - b. Agency shall pay for the Services as set forth in the applicable Schedule(s) attached hereto. Pricing set forth in the applicable Schedule is based on one use/decision per transaction. A Schedule may be modified by EVS upon thirty (30) days’ notice. Agency’s use of the Service after such thirty (30) day period shall constitute its agreement to such change(s), without prejudice to its right to terminate this Agreement as provided in Section 7 below.
 - c. Agency certifies that it will order Data from the Service only when Agency 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) solely 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) in connection with a determination of the 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, (5) when Agency 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 (6) for employment purposes.
 - d. Agency 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”) Notice Form attached as Exhibit 1.
 - e. Agency 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 Agency may obtain Data for employment purposes and will also obtain the Consumer’s written authorization to obtain or procure Data relating to that Consumer.

- f. Agency 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.
- g. Agency acknowledges that it has received from EVS a copy of the consumer rights summary as prescribed by the CFPB (see Exhibit 3).
- h. Agency certifies that it will comply with applicable provisions under Vermont law. In particular, Agency certifies that it will order Data relating to Vermont residents only after Agency has received prior Consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Agency further certifies that the attached copy of VFCRA Section 2480e applicable Vermont Rules as referenced in Exhibit 2 was received from EVS.
- i. Agency may use the Data provided through the Service only as described in this Agreement. Agency 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 Agency first obtains EVS's written consent; provided, however, that Agency may discuss Consumer Data with the Data subject when Agency has taken adverse action against the subject based on the Data. Agency 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. Agency will refer the Consumer to EVS whenever the Consumer disputes the Data disclosed by Agency. Agency 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. Agency 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"). Agency 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 Agency first obtaining EVS's written permission.
- g. Agency represents it (i) is administering a government funded benefit or program, (ii) has been given the legal authority to view the Data by the Consumer or by operation of law, and (iii) is requesting the Data in compliance with all laws.
- h. Agency acknowledges it shall employ decision making processes reasonable and appropriate to the nature of the transaction and will utilize the Data as part of its process.
- i. Agency represents it has authorization from the Consumer to verify income. Agency need not use any particular form of authorization or obtain a separate signature for verifying income provided the form is auditable and demonstrates to a reasonable degree of certainty that the Consumer has authorized the Agency to obtain the income Data. Notwithstanding the foregoing, in the event Agency is using the Service to collect on defaulted child support obligations, Agency is not required to obtain such authorization.
- j. Agency 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 and without the Service Provider first entering into a separate agreement with EVS.
- k. In order to ensure compliance with this Agreement, applicable law and EVS policies, EVS may conduct reviews of Agency activities, from time to time, during normal business hours, at all locations containing relevant records, with respect to Agency's requests for Data and/or its use of Data. Agency shall provide documentation within a reasonable time to EVS as reasonably requested for purposes of such review. Agency (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). Agency shall include the name and email address of the appropriate point of contact to whom such request should be made in the space provided below. Agency may change its contact information upon written notice:

| Audit Contact Name | Audit Contact E-mail Address |
|--------------------|------------------------------|
| | |

I. Additional representations and warranties as may be set forth in each Schedule A.

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

a. Agency 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 Agency 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 security procedures and controls which are standard practice in the data protection industry (“Industry Standard Practices”), for example compliance with ISO 27001 standards,
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 Agency security codes, user names, User IDs, and any passwords Agency 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 Agency passwords at least every ninety (90) days or sooner if Agency suspects an unauthorized person has learned the password; and perform at a minimum, quarterly entitlement reviews to recertify and validate Authorized User’s access privileges and disable the account of any Agency user who is no longer responsible for accessing the Service,
7. adhere to all security features in the software and hardware Agency 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-agency 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, Industry Standard Practices for the type of Data received from EVS must be employed,

11. if Agency 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 Agency's locations or to third parties without deleting all EVS Agency number(s), security codes, User IDs, passwords, Agency user passwords, and any consumer information, or Data,
 13. monitor compliance with the obligations of this Section, and immediately notify EVS if Agency 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, Agency uses a Service Provider to establish access to the Service, be responsible for the Service Provider's use of Agency's user names, security access codes, or passwords, and Agency will ensure the Service Provider safeguards Agency's security access code(s), User IDs, and passwords through the use of security requirements that are no less stringent than those applicable to Agency under this Section,
 15. use Industry Standard Practices 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 Agency'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 Industry Standard Practices 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) Data must be protected through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iii) access (both physical and network) to systems storing Data must be secure, 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 Industry Standard Practices 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 Agency has a security incident involving EVS Confidential Information, Agency will fully cooperate with EVS in a security assessment process and promptly remediate any finding.
- b.** If EVS reasonably believes that Agency has violated this Section, EVS may, in addition to any other remedy authorized by this Agreement, with reasonable advance written notice to Agency and at EVS's sole expense, conduct, or have a third party conduct on its behalf, an audit of Agency's network security systems, facilities, practices and procedures to the extent EVS reasonably deems necessary, including an on-site inspection, to evaluate Agency's compliance with the data security requirements of this Section.

- 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, 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 any other 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 with respect to (i) 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) 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. TERM AND TERMINATION.** This Agreement shall be for an annual term, and shall automatically renew for successive one year terms. Either EVS or Agency may terminate this Agreement or any Schedule(s), at any time upon thirty (30) days’ prior written notice to the other. If EVS believes that Agency 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 Agency.
- 7. RIGHTS TO SERVICE.** The Service and the Data, including all rights thereto, are proprietary to EVS.
- 8. 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. Agency 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.
- 9. INDEMNIFICATION.** Agency 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. To the extent permitted by laws applicable to the parties, 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. Further, each party agrees to Indemnify the other from and against the Indemnifying Party’s (i) violation of applicable law, or (ii) breach of Confidentiality obligations.
- 10. LIMITATION OF LIABILITY.** 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 performance of this Agreement, even if that party has been advised of the possibility of such damages. In no event shall damages of any kind payable by EVS hereunder exceed the sum paid by Agency for the item of service which causes Agency’s claim.

11. 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.

12. 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 Agency 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 Agency 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 personal 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.

13. COUNTERPARTS/EXECUTION BY FACSIMILE. For the convenience of the parties, copies of this Agreement and Schedules hereof may be executed in two or more counterparts and signature pages exchanged by facsimile. The parties intend that counterpart copies signed and exchanged as provided in the preceding sentence shall be fully binding as an original handwritten executed copy hereof and thereof and all of such copies together shall constitute one instrument.

By signing below, Agency acknowledges receipt of Exhibit 1, "Notice to Users of Consumer Reports Obligations of Users"; and Agency represents that Agency has read "Notice to Users of Consumer Reports Obligations of Users" which explains Agency's obligations under the FCRA as a user of consumer report information

IN WITNESS WHEREOF, the parties have executed this Agreement on the date indicated below.

Agency

**TALX Corporation,
provider of Equifax Verification Services**

By
(signature): _____
Name
(print): _____
Title: _____
Date: _____

By
(signature): _____
Name
(print): _____
Title: _____
Date: _____

UNIVERSAL MEMBERSHIP AGREEMENT
for
The Work Number[®] for Government Agencies

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[®] for Government Agencies

Exhibit 2

VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION

The undersigned, _____ (“Agency”), 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 Agency's continued use of EVS services in relation to Vermont consumers, Agency hereby certifies as follows:

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

Agency: _____

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[®] for Government Agencies

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 & 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> |

Contact Us

Primary Contact

Kurt D. Jones

Account Executive

Equifax Government Services

O 314-214-7080

C 314-941-2677

kurt.jones@equifax.com

Equifax Workforce Solutions

11432 Lackland Road

St. Louis, MO 63146

www.equifax.com/workforce