

&lt; SFDC - GTM Account Name &gt;

EXECUTABLE LRD: 04/26/2024

EFXID:

CUS-24-49908 - Texas General Land Office

**UNIVERSAL MEMBERSHIP AGREEMENT****for****Equifax Verification Services****("Company" or "GLO"):** Texas General Land Office and Veterans Land Board**Company's Address:** 1700 N. Congress Avenue, Austin, TX 78701**Effective date of this Universal Membership Agreement ("Effective Date"):** May 1, 2024

(If blank, the Effective Date of this Universal Membership Agreement shall be the date of the last signature below).

This **Universal Membership Agreement (otherwise known as GLO Contract No. 24-134-000-E464)** (the "Agreement" or "Contract"), effective as of the Effective Date, is entered into by and between Equifax Workforce Solutions LLC, a Missouri limited liability company and provider of Equifax Verification Services located at 11432 Lackland Road, St. Louis, Missouri 63146 ("EVS" or "Provider"), and Company.

**RECITALS:**

- A. EVS operates The Work Number® ("TWN"), a service used to verify employment and income information about an individual ("Consumer"), and various other services ("EVS Services") used to verify certain Consumer information (TWN and EVS Services are collectively referred to herein as the "Service"); and
- B. Company 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, Exhibit 1, Exhibit 2, Exhibit 3, the EVS Security Exhibit attached hereto, 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. For the avoidance of doubt, the parties agree that upon execution of this Agreement, the Universal Membership Agreement between Texas General Land Office and Veterans Land Board and TALX Corporation effective as of May 1, 2021, as amended, and all accompanying schedules shall be terminated and are of no further force or effect.
2. **EVS OBLIGATIONS.** TWN will provide Company with automated access to certain employment and/or income data ("Data") furnished to EVS by employers, and the EVS Services will provide Company with access to certain other information ("Information") as described in each Schedule A attached hereto.
3. **COMPANY OBLIGATIONS.**
  - a. Company shall comply with the terms set forth in this Agreement, and each Exhibit and Schedule attached hereto.
  - b. Company shall pay for the Services as set forth in each applicable Schedule. All prices stated in any Schedule attached to this Agreement are exclusive of sales, use, privilege, or excise taxes. Applicable sales, use, privilege, or excise taxes shall be included in each invoice, except as otherwise exempted in the applicable Schedule.
  - c. Company certifies that it will order Data from TWN only when Company (i) intends to use the Data 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) has obtained 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 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 (6) 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.
  - d. 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.

- e. 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. NO PROVISION IN THIS AGREEMENT, INCLUDING ANY EXHIBITS ATTACHED HERETO OR INCORPORATED HEREIN, SHALL BE CONSTRUED AS A WAIVER OF THE COMPANY'S SOVEREIGN IMMUNITY. To the extent that this Agreement, including any exhibits attached hereto or incorporated herein, imposes any requirement to comply with the laws of any other state or local government, such requirement shall be limited to the extent allowable under Texas law.
- f. Section 1785.14(a) of the California Civil Code imposes special requirements with respect to transactions in which a "retail seller" (as defined in Section 1802.3 of the California Civil Code) intends to issue credit to a California resident who appears in person on the basis of an application for credit submitted in person ("point of sale transactions"). Company certifies that these requirements do not apply to it because Company is NOT a "retail seller" (as defined in Section 1802.3 of the California Civil Code), and/or (b) Company does NOT issue credit to California residents who appear in person on the basis of applications for credit submitted in person. Company further certifies that it will notify EVS in writing 30 days PRIOR to becoming a retail seller or engaging in point of sale transactions with respect to California residents.
- g. Company will comply with the provisions of the FCRA, the Federal Equal Credit Opportunity Act, as amended, all state law counterparts of them, including applicable Texas law, and all applicable regulations promulgated under any of them, including, without limitation, any provisions requiring adverse action notification to the Consumer.
- h. Company may use the Data and Information provided through the Service only as described in this Agreement. Company may reproduce or store the Data and Information obtained from the Service solely for its own use in accordance with this Agreement, and will hold all Data and Information 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 permitted in this Agreement, required by law, or 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.
- i. 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 and Information as part of its processes.
- j. "Processing" means accessing (including access to view), transmitting, using, or storing the Services, and any Data or Information provided or obtained through the Services (the "EVS Information"). Company may Process EVS Information from the United States, Canada, and the United States territories of American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U. S. Virgin Islands (collectively, the "Permitted Territory"). Company must (i) notify EVS thirty (30) days prior to Processing EVS Information from a location outside of the Permitted Territory, in accordance with the notice requirements described in this Agreement; and (ii) sign an International Access and Use Addendum with EVS prior to Processing EVS Information from a location out of the Permitted Territory. EVS reserves the right to deny any such request for reasons including, without limitation, regulatory requirements, security concerns, or existing contractual obligations. Notwithstanding the foregoing, Company is prohibited from Processing EVS Information from an Embargoed Country. "Embargoed Country" means any country or geographic region subject to comprehensive economic sanctions or embargoes administered by OFAC or the European Union.
- k. Except as otherwise permitted in Section 5.b. below, Company may not allow a third party service provider (hereafter "Service Provider") to access, use, or store the Data or Information on its behalf without first obtaining EVS's written permission, which such permission shall not be unreasonably withheld or denied, and without the Service Provider first entering into a separate agreement with EVS.
- l. 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 or Information and/or its use of Data or Information. Company shall provide documentation within a reasonable time to EVS as reasonably requested for purposes of such review. Company 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). Company 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). Company 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. Company may change its contact information upon written notice:

Audit Contact Name	Audit Contact E-mail Address
Kimilia Mangum	kimilia.mangum@glo.texas.gov

4. **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 and Information obtained from the Service, 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 or as may be required, governed, or protected

by any other applicable law or legal process. Nothing in this section shall preclude or impede the Agency from fulfilling any and all obligations under the Texas Public Information Act, including submission via the Agency's Office of General Counsel to the Office of the Attorney General of the State of Texas' Open Records Division. 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 4, 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.

**5. DATA SECURITY.** This Section 5 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 5, 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 or Information 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 or Information for personal reasons or provide Data or Information 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 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 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 passwords according to NIST 800-63.3B, or sooner if Company 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 Company user who is no longer responsible for accessing the Service;
7. leverage advanced authentication mechanism such as multifactor authentication;
8. adhere to all security features in the software and hardware Company uses to order or access the Services, including the use of IP restriction;
9. 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;
10. in no event access the Services via any unregistered wireless hand-held communication device, that have not gone through Company's device enrollment, access, and authentication process. Such process shall be reviewed and approved by EVS prior to allowing access to Services via any hand-held communication device;
11. 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 or Information. In addition, Data and Information must be encrypted when not in use and all printed Data and Information 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 and Information received from EVS must be employed;
12. if Company sends, transfers or ships any Data or Information, encrypt the Data and Information using the following minimum standards, which standards may be modified from time to time by EVS: TLS 1.2+ for Data in transit; and AES-128 BIT for Data while at rest;
13. not ship hardware or software between Company's locations or to third parties without deleting all of EVS's Confidential Information, Company number(s), security codes, User IDs, passwords, Company user passwords, and any Consumer information, or Data;
14. monitor compliance with the obligations of this Section 5, 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;

15. 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 5;
  16. use Industry Standard Practices to assure data security when disposing of any Data and Information 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;
  17. use Industry Standard Practices to secure Data and Information when stored on servers, subject to the following requirements: (i) servers storing Data and Information 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 and Information 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 and Information must be secure, which must include authentication and passwords that are changed according to NIST 800-63.3B; and (iv) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available;
  18. not allow Data or Information to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices;
  19. 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;
  20. 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
  21. 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. For purposes of this Section 5, "**Security Incident**" means any actual breach, theft or unauthorized access, use, misuse, theft, vandalism, modification or transfer of or to Services or Data.
- b. A cloud service provider ("**CSP**") is a company that offers a component of cloud computing. CSPs generally offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). Company may use a CSP to process, transmit, or store Data and Information, subject to the requirements below.
1. Company may use Amazon Web Services, Google Cloud Platform, Microsoft Azure, or Salesforce exclusively as their CSP, so long as Company certifies its CSP has the following minimum requirements: (i) Data and Information at rest is encrypted at a minimum of AES-256; (ii) Data and Information shall be encrypted in transit both internally and externally at a minimum of TLS version 1.2 and/or AES-128; (iii) Company shall manage all encryption keys within the Company's CSP; (iv) an inventory shall be kept of all Data and Information within the cloud environment; (v) Data and Information shall be logically and/or physically separated in multi-tenant environments in accordance with industry standards; and (vi) access control standards that include: user provisioning, regular access reviews, password requirements, need to know permissions, and least privilege principles.
  2. For all other CSPs, Company certifies that Company will, and will contractually obligate its CSP to, follow EVS's minimum requirements: (i) Data and Information at rest is encrypted at a minimum of AES-256; (ii) Data and Information shall be encrypted in transit both internally and externally at a minimum of TLS version 1.2 and/or AES-128; (iii) Company shall manage all encryption keys within the Company's CSP; (iv) an inventory shall be kept of all Data and Information within the cloud environment; (v) Data and Information shall be logically and/or physically separated in multi-tenant environments in accordance with industry standards; (vi) access control standards that include: user provisioning, regular access reviews, password requirements, need to know permissions, and least privilege principles; (vii) utilization of secure data destruction techniques shall be used to destroy Data and Information in accordance with industry standards; (viii) assets that are no longer needed for legal purposes shall be destroyed in accordance with industry standard; (ix) incident handling and forensic support shall be provided in the event of an investigation or Security Incident; (x) cloud hosted systems shall be patched at the most current levels and have vulnerabilities addressed in accordance with industry standards; (xi) information systems and infrastructures shall follow industry security hardening standard such as DISA STIG or CIS guidance; (xii) CSP's application environment shall be certified by an independent third party (SOC 2 Type 2), if operating in a hybrid environment, a SOC 2 Type 2 or equivalent shall also be required for the Company; (xiii) Third parties providing support services to the Company or Company's CSP shall not have access to Data and Information without prior consent of EVS; (xiv) CSP shall have network-based Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) tools deployed in or around the cloud network infrastructure; (xv) centralized logging and monitoring of the CSP's infrastructure/environment; and (xvi) Company shall utilize multi-factor authentication (MFA) to remotely access CSP's infrastructure/environment.
- c. If EVS reasonably believes Company has violated this Section 5, 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 facilities, security 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 5.
6. **TERM.** This Agreement shall be for an initial term of one (1) year (the "Initial Term"), effective as of the Effective Date of May 1, 2024 to April 30, 2025, and may be extended for three (3) discrete annual terms ("Renewal Term(s)"), with pricing reflected in the applicable Schedule A, to be negotiated and mutually agreed upon each year to the next, given the Company's budget authority. Renewal Terms must be requested by Company at least thirty (30) days in advance of the then-applicable expiration date. In no event will this Agreement remain in effect after April 30, 2028.

## 7. Termination.

7.1 The GLO may, in its sole discretion, terminate the Contract upon thirty (30) days' written notice to Provider by email, facsimile, or certified mail return receipt requested and is effective upon Provider's receipt. In the event of such termination, Provider shall, unless otherwise mutually agreed upon in writing, cease all work immediately upon the effective date of termination. The GLO shall be liable for payments for any goods or services delivered by Provider as set forth in the applicable Schedule. If Provider fails to provide the goods or services contracted for according to the provisions of the Contract, or fails to comply with any terms or conditions of the Contract, the GLO must give EVS at least thirty (30) days prior written notice in which to cure the breach before terminating the Contract. If EVS fails to cure within thirty (30) days following such written notice, GLO may, upon written notice of default to Provider, immediately terminate all or any part of the Contract. Termination is not an exclusive remedy, but will be in addition to any other rights and remedies as provided in equity, by law or under the Contract.

7.2 **Abandonment.** Additionally, if Provider abandons on the Contract, the GLO may terminate the Contract without notice and either re-solicit or re-award the Contract to the next best responsive and responsible provider. The defaulting Provider will not be considered in the re-solicitation and may not be considered in future solicitations for the same type of work, unless the specification or scope of work significantly changed. The period of suspension will be determined by the GLO based on the seriousness of the abandonment.

7.3 The parties may exercise any other right, remedy, or privilege which may be available to it under applicable law.

7.4 EVS may terminate this Agreement or any Schedule(s), at any time upon thirty (30) days' prior written notice to the Company.

7.5 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 if such breach is not resolved within thirty (30) days of notice. Notwithstanding, EVS may suspend Company's use of the Services upon notice during any such cure period in order for Company to remediate any such violation. In addition, if EVS reasonably believes that Company has violated any Data use, or Data security restriction required by this Agreement, EVS may, at EVS' option and reserving all other rights and remedies, suspend this Agreement and/or any Schedules immediately upon notice to Company.

8. **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.

9. **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.

10. **FORCE MAJEURE.** Neither Provider nor the GLO shall be liable to the other for any delay in, or failure of performance, of any requirement in any Schedule or Purchase Order resulting from the Contract caused by force majeure. Such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed, provided the non-performing party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failures of transportation, or other causes that are beyond the reasonable control of either party and that by exercise of due foresight such party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such party is unable to overcome. Each party must inform the other in writing, which may include electronic mail, with proof of receipt, promptly, of the existence of such force majeure, or otherwise waive this right as a defense. Notwithstanding anything herein to the contrary, neither Party shall be relieved of its obligations to pay amounts owed to the other that are delinquent or past due prior to the force majeure event date.

11. **INDEMNIFICATION – Acts/Omissions.** Provider shall indemnify, defend, and hold harmless the State of Texas, the GLO, and/or their officers, agents, employees, and representatives, contractors, assignees, and/or designees from and against any and all liability, actions, claims, demands, damages, proceedings, or suits, and all reasonably related costs, attorney fees, and expenses arising out of, connected with, or resulting from any acts or omissions of Provider or its officers, agents, employees, representatives, suppliers, contractors, subcontractors, assignees, designees, order fulfillers, or suppliers of contractors or subcontractors in the execution or performance of the Contract and any Schedules or Purchase Orders issued under the Contract. Provider and the GLO shall furnish timely written notice to each other of any such claim. Provider shall be liable to pay all costs of defense, including attorneys' fees. Provider shall coordinate its defense with the Office of the Attorney General when Texas state agencies are named defendants in any lawsuit and Provider may not agree to any settlement without first obtaining the written consent of the Office of the Attorney General. THIS PARAGRAPH IS NOT INTENDED AND SHALL NOT BE CONSTRUED TO REQUIRE EVS TO INDEMNIFY OR HOLD HARMLESS THE STATE OF TEXAS OR THE GLO, FOR CLAIMS OR LIABILITIES RESULTING FROM THE NEGLIGENT ACTS OR OMISSIONS OF GLO OR ITS EMPLOYEES. FOR THE AVOIDANCE OF DOUBT, THE GLO SHALL NOT INDEMNIFY EVS OR ANY OTHER ENTITY UNDER THIS AGREEMENT.

## 12. Infringement Including Indemnity.

a) Provider shall indemnify, defend, and hold harmless the State of Texas, the GLO, and/or their officers, agents, employees, representatives, contractors, assignees, and/or designees from and against any and all liability, actions, claims, demands, damages, proceedings, or suits, and all related costs, attorney fees, and expenses arising out of, connected with, or resulting from infringement of any United States patent, copyright, trade or service mark, or any other intellectual or intangible property right that occurs in the execution or performance of the Contract and any Schedules or Purchase Orders issued under the Contract. Provider and the GLO shall furnish timely written notice to each other of any such claim. Provider shall be liable to pay all costs of defense including attorneys' fees. Provider shall coordinate its defense with the Office of the Attorney General when Texas state agencies are named defendants in any lawsuit and Provider may not agree to any settlement without first obtaining the written consent of the Office of the Attorney General.

b) Provider shall have no liability under this section if the alleged infringement is caused in whole or in part by: (i) use of the product or service for a purpose or in a manner for which the product or service was not designed, (ii) any modification made to the product without Provider's written approval, (iii) any modifications made to the product by the Provider pursuant to GLO's specific instructions, or (iv) any use of the product or service by GLO that is not in conformity with the terms of the Contract or any applicable license agreement.

c) If Provider becomes aware of an actual or potential claim, or the GLO provides Provider with notice of an actual or potential claim, Provider may (or in the case of an injunction against the GLO, shall), at Provider's sole option and expense; (i) procure for the GLO the right to continue to use the affected portion of the product or service, or (ii) modify or replace the affected portion of the product or service with a functionally equivalent or superior product or service so that the GLO's use is non-infringing.

### 13. Taxes, Workers Compensation, Unemployment Insurance – Including Indemnity.

(a) Provider shall be solely liable and responsible for payment of Provider's and Provider's employees' taxes of whatever kind, arising out of the execution or performance of the Contract. Provider shall comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and workers' compensation. The GLO and the State of Texas shall not be liable to Provider or its officers, agents, employees, representatives, contractors, assignees, designees, or others for the payment of taxes, or the provision of unemployment insurance, workers' compensation, or any benefit available to a state employee or employee of another governmental entity.

(b) Provider shall indemnify, defend, and hold harmless the State of Texas, the GLO, and/or their officers, agents, employees, representatives, contractors, assignees, and/or designees from and against any and all liability, actions, claims, demands, damages, proceedings, or suits, and all related costs, attorney fees, and expenses arising out of, connected with, or resulting from tax liability, unemployment insurance, or workers' compensation in the execution or performance of the Contract and any Schedules or Purchase Orders issued under the Contract. Provider and the GLO shall furnish timely written notice to each other of any such claim. Provider shall be liable to pay all costs of defense including attorneys' fees. Provider shall coordinate its defense with the Office of the Attorney General when Texas state agencies are named defendants in any lawsuit and Provider may not agree to any settlement without first obtaining the written consent of the Office of the Attorney General.

(c) The GLO is exempt from federal, state, and local taxes. Provider shall not charge any taxes to the GLO.

### 14. LIMITATION OF LIABILITY. EVS' LIABILITY UNDER THIS AGREEMENT, FOR ANY AND ALL CLAIMS ARISING OUT OF, OR RELATED TO, THIS AGREEMENT, SHALL NOT EXCEED THE AMOUNT ACTUALLY RECEIVED BY EVS FROM COMPANY FOR THE SERVICE CONNECTED WITH THE EVENT WHICH GAVE RISE TO LIABILITY. THE FOREGOING EXCLUSIONS OF LIABILITY SHALL NOT APPLY TO: (I) EVS' INDEMNIFICATION OBLIGATIONS SET FORTH IN THIS AGREEMENT; (II) EVS' BREACH OF ITS CONFIDENTIALITY AND DATA SECURITY OBLIGATIONS SET FORTH IN THIS AGREEMENT; (III) EVS' BREACH OF APPLICABLE LAWS; OR (IV) CLAIMS OR DAMAGES ARISING FROM EVS' WILLFUL MISCONDUCT OR FRAUD.

IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY UNDER ANY THEORY OR CIRCUMSTANCE FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES.

### 15. INSURANCE – During the term of the Agreement, EVS shall maintain the following insurance with insurance companies with a minimum Best's rating of A- VIII:

**Workers' Compensation** - (A) Workers' Compensation Limit: Statutory and (B) Employer's Liability: (1) Bodily Injury by Accident, for Each Accident: \$1,000,000 (2) Bodily Injury for Each Employee by Disease: \$1,000,000 and (C) Policy Limit for Bodily Injury by Disease: \$1,000,000;

**General Liability** - Policy will include coverage for bodily injury, property damage, personal injury, advertising injury, contractual liability, products/completed operations. (A) Per Occurrence Limit: \$1,000,000 (B) General Aggregate: \$2,000,000; Agency, its officers, employees, and authorized agents will be listed as additional insureds where required by written contract. This additional insured endorsement may be blanket or automatic and Equifax's insurance shall be primary and non-contributory;

**Automobile Liability** - Policy will include coverage for all owned, non-owned, and hired vehicles used by Equifax in the performance of the Services. Limit: \$1,000,000. Agency, its officers, employees, and authorized agents will be listed as additional insureds where required by written contract. This additional insured endorsement may be blanket or automatic and Equifax's insurance shall be primary and non-contributory;

**Umbrella Liability** - Policy provides additional limits excess of Employer's Liability, General Liability and Automobile Liability policies. Limit: \$5,000,000;

**Professional Liability (a/k/a Errors & Omissions Insurance) including Network Security & Privacy Liability (a/k/a Cyber)**- Policy will include coverage for actual or alleged breach of duty, act, error, omission, misstatement, misleading statement or neglect in the rendering of or failure to render the services under this Agreement. Policy will also include coverage for liability as a result of a data security breach or violation of consumer data protection laws. The professional liability insurance and network security and privacy liability insurance may be maintained under a combined policy or via separate policies. Aggregate Limit: \$1,000,000; If the coverage is maintained on a claims made basis, the policy will include an extended reporting period of one (1) year if reasonably available in the commercial marketplace.

Insurance Certificates must:

- (a) be submitted to insurance@GLO.TEXAS.GOV
- (b) prominently display "GLO Contract No.24-134-000-E464."; and
- (c) Name the Agency as an additional insured.

Prior to commencement of Services, EVS shall provide a certificate of insurance to Agency evidencing each of the insurance policies above. Renewal certificates can also be provided to Agency. In addition, EVS will endeavor to provide thirty (30) days' notice of cancellation or non-renewal.

16. **Prohibited Benefits.** Pursuant to Section 2155.003 of the Texas Government Code, Provider represents and warrants that it has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with the Contract.
17. **Prohibited Financial Participation.** Pursuant to Section 2155.004(a) of the Texas Government Code, Provider certifies that neither Provider nor any person or entity represented by Provider has received compensation from the GLO to participate in the preparation of the specifications or solicitation on which this Contract is based. Under Section 2155.004(b) of the Texas Government Code, Provider certifies that the individual or business entity named in this Contract is not ineligible to receive the specified contract and acknowledges that the Contract may be terminated and payment withheld if this certification is inaccurate. This Section does not prohibit Provider or a contract participant from providing free technical assistance.
18. **Texas Resident Bidder.** Provider certifies that if its business address shown on the Contract is a Texas address, that address is the legal business address of Provider and Provider qualifies as a Texas Resident Bidder under Texas Administrative Code, Title 34, Part 1, Chapter 20.
19. **Delinquent Child Support.** Under Section 231.006(d) of the Texas Family Code, regarding child support, Respondent certifies that the individual or business entity named in this Response is not ineligible to receive the specified payment and acknowledges that the contract may be terminated and payment may be withheld if this certification is inaccurate. Furthermore, any Respondent subject to Section 231.006 of the Texas Family Code, must include in the Response the names and social security numbers of each person with at least 25% ownership of the business entity submitting the Response.
20. **Executive Head of State Agency.** In accordance with Section 669.003 of the Texas Government Code relating to contracting with the executive head of a state agency, Provider certifies that it (1) is not the executive head of the GLO; (2) was not, at any time during the four years before the effective date of the Contract, the executive head of the GLO; and (3) does not employ a current or former executive head of the GLO.
21. **Debt.** EVS agrees that any payments due under the Contract shall be applied towards any debt or delinquency that is owed to the State of Texas.
22. **Excluded Parties.** Provider certifies that it is not listed in the prohibited vendors list authorized by Executive Order No. 13224, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism", published by the United States Department of the Treasury, Office of Foreign Assets Control.
23. **Suspension and Debarment.** Provider certifies that neither it nor its principals are debarred, suspended, proposed for debarment, declared ineligible, or otherwise excluded from participation in the Contract by any state or federal agency.
24. **Convictions or Penalties in Connection with Hurricanes Rita and Katrina.** Sections 2155.006 and 2261.053 of the Texas Government Code, prohibit state agencies from accepting a Response or awarding a contract that includes proposed financial participation by a person who, in the past five years, has been convicted of violating a federal law or assessed a penalty in connection with a contract involving relief for Hurricane Rita, Hurricane Katrina, or any other disaster, as defined by Section 418.004 of the Texas Government Code, occurring after September 24, 2005. Under Sections 2155.006 and 2261.053 of the Texas Government Code, Provider certifies that the individual or business entity named in this Contract is not ineligible to receive the specified contract and acknowledges that this Contract may be terminated immediately, and payment withheld if this certification is inaccurate.
25. **State's Right to Audit Provider.** The state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under the Contract or indirectly through a subcontract under the Contract. Acceptance of funds directly under the Contract or indirectly through a subcontract under the Contract acts as acceptance of the authority of the state auditor, under the direction of the legislative audit committee, to conduct an audit or investigation in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit, subject to Contractor's reasonable onsite security practices over its facilities and in accordance with Section 13 of the Security Exhibit. Provider shall ensure that this clause concerning the authority to audit funds received indirectly by subcontractors through Provider and the requirement to cooperate is included in any subcontract it awards specifically for the purpose of providing Services under the Contract.
26. **Antitrust.** Provider represents and warrants that, in accordance with Section 2155.005 of the Texas Government Code, neither Provider nor the firm, corporation, partnership, or institution represented by Provider, nor anyone acting for such a firm, corporation, partnership, or institution has (1) violated any provision of the Texas Free Enterprise and Antitrust Act of 1983, Chapter 15 of the Texas Business and Commerce Code, or the federal antitrust laws, or (2) communicated directly or indirectly the contents of this Contract or any solicitation response upon which this Contract is based to any competitor or any other person engaged in the same line of business as Provider. Additionally, Provider hereby assigns to Company, Provider's rights, title, and interest in and to all claims and causes of action Provider may have under the antitrust laws of Texas for overcharges specifically related to and associated with this Contract and Company, for the item of Service rendered therein which creates the cause of action in question.
27. **APPLICABLE LAW; Venue; Sovereign Immunity.** This Contract shall be governed by and construed in accordance with the laws of the State of Texas. Except as provided by applicable statute, Venue for any suit arising under this Contract is fixed in any court of competent jurisdiction of Travis County, Texas. Neither the Contract, nor any conduct of any GLO representative, shall be construed to waive sovereign immunity on behalf of the GLO or the State of Texas.
28. **Preference for Texas Products and Materials.** To the extent applicable, in accordance with Section 2155.4441 of the Texas Government Code, Provider agrees that during the performance of a contract for services it shall purchase products and materials produced in Texas when they are available at a price and time comparable to products and materials produced outside Texas.

- 29. Public Information.** Provider understands that the GLO will comply with the Texas Public Information Act (Chapter 552 of the Texas Government Code) as interpreted by judicial rulings and opinions of the Attorney General of the State of Texas. Information, documentation, and other material in connection with this Contract may be subject to public disclosure pursuant to the Texas Public Information Act. In accordance with Section 2252.907 of the Texas Government Code, Provider is required to make any information created or exchanged with the State pursuant to the Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.
- 30. Dispute Resolution.** Except as otherwise provided by statute, rule, or regulation, the dispute resolution process provided for in Chapter 2260 of the Texas Government Code must be used to attempt to resolve any dispute arising under the Contract that cannot be resolved by the parties in the ordinary course of business. NOTHING IN THIS SECTION SHALL BE CONSTRUED AS A WAIVER OF SOVEREIGN IMMUNITY BY THE GLO.
- 31. Funding Out Clause.** This Contract is contingent upon the continued availability of lawful appropriations by the Texas Legislature. Provider understands that all obligations of the GLO under the Contract are subject to the availability of state funds. If such funds are not appropriated or become unavailable, the GLO shall provide Contractor with commercially reasonable notice and may terminate the Contract. However, failure by the GLO to provide such commercially reasonable notice shall not be considered a breach of contract on behalf of the GLO. The Contract shall not be construed as creating a debt on behalf of the GLO in violation of Article III, Section 49a of the Texas Constitution.
- 32. Independent Contractor.** Provider and its employees, representatives, agents, and subcontractors, if applicable, shall serve as an independent contractor in the performance of the Contract. Provider and its employees, representatives, agents, and subcontractors shall not be employees of the GLO by virtue of the Contract. Should Provider subcontract any of the services required under the Contract, Provider agrees the GLO is not liable to any subcontractor(s) of Provider. This provision does not relieve Provider of the responsibility for ensuring that the services rendered under all subcontracts are rendered in compliance with the Contract.
- 33. Records Retention.** Provider shall maintain all records that may demonstrate payments under the Contract were expended in accordance with the laws and regulations of the State of Texas. Provider shall maintain all such records for a period of seven (7) years after the date of submission of the final invoices or until a resolution of all billing questions, whichever is later. Provider shall make available at reasonable times during normal business hours, and upon reasonable notice for reasonable periods, subject to Contractor's reasonable onsite security practices over its facilities and systems and in accordance with Section 13 of the Security Exhibit, all documents and other information related to the Contract. Provider shall provide the State Auditor with any information that the State Auditor deems relevant to any investigation or audit. Provider must retain all work and other supporting documents pertaining to the Contract, for purposes of inspections, monitoring, audits, or evaluations by the GLO and any authorized agency of the State of Texas, in accordance with applicable law.
- 34. Payment.** Provider shall submit invoices to the GLO for delivered goods or completed services not later than the 15th day of the month after delivery or completion. The GLO shall make no payments without Provider's prior submission of detailed, correct invoices. The GLO shall make payments in accordance with Texas Government Code Chapter 2251. Payments under this Contract are subject to the availability of appropriated funds. Provider acknowledges and agrees that payments for services provided under this Contract are contingent upon the GLO's receipt of funds appropriated by the Texas Legislature. **ALL Provider invoices shall: 1) be submitted via email to [VendorInvoices@GLO.TEXAS.GOV](mailto:VendorInvoices@GLO.TEXAS.GOV); 2) be supported by documentation that, in the judgment of the GLO, allows for full substantiation of the costs incurred; and 3) prominently display "GLO Contract No. 24-134-000-E464". If Provider does not submit invoices in strict accordance with the instructions in this section, payment of invoices may be significantly delayed. Provider agrees that the GLO shall not pay interest, fees, or other penalties for late payments resulting from Provider's failure to submit invoices in strict accordance with the instructions in this section.**
- 35. Severability.** If a court of competent jurisdiction determines any term or condition herein or any provision of the Contract is invalid, void, or unenforceable, the remaining terms, provisions, covenants, and conditions shall remain in full force and effect, and shall in no way be affected, impaired, or invalidated.
- 36. Fraud.** The GLO does not tolerate any type of fraud. GLO policy promotes consistent, legal, and ethical organizational behavior by assigning responsibilities and providing guidelines to enforce controls. Any violations of law, agency policies, or standards of ethical conduct will be investigated, and appropriate actions will be taken. Provider shall report any possible fraud, waste, or abuse that occurs in connection with the Contract to GLO as directed by the GLO's website, <http://glo.texas.gov>.
- 37. Israel Boycott.** If Chapter 2271 of the Texas Government Code applies to this Contract, Provider verifies it does not boycott Israel and will not boycott Israel during the term of this Contract.
- 38. Prohibited Business Engagements.** Provider represents and warrants that it is not engaged in business with Iran, Sudan, or a foreign terrorist organization, as prohibited by Section 2252.152 of the Texas Government Code.
- 39. Continuity and Disaster Recovery Plans.** Provider has noted its most recent business continuity and disaster recovery obligations as set forth in the Security Exhibit to the Contract attached hereto.
- 40. False Statements or Material Misrepresentations.** Provider represents and warrants that all statements and information prepared and submitted in this document are current, complete, true, and accurate. Submitting a false statement or making a material misrepresentation during the performance of a contract is a material breach of contract and may void the Contract or constitute grounds for its termination.
- 41. Conflicts of Interest.** EVS represents and warrants that the provision of goods and services or other performance under the Contract will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.
- 42. Signature Authority.** The person signing the Contract on behalf of each party certifies they are 1) duly authorized to execute the Contract on their own behalf or on behalf of its party and 2) legally empowered to contractually bind its party to the Contract and related documents.
- 43. Survival of Terms and Conditions.** The terms and conditions herein and in the Contract shall survive the termination or expiration of the Contract.



- 44. Contracting Information.** To the extent Section 552.371 of the Texas Government Code applies to Provider and the Contract, Provider represents and warrants that Provider will comply with the requirements of Section 552.372(a) of the Texas Government Code. Except as provided by Section 552.374(c) of the Texas Government Code, the requirements of Subchapter J, Chapter 552 of the Government Code, may apply to the Contract and Provider agrees that the Contract can be terminated if Provider knowingly or intentionally fails to comply with a requirement of that subchapter.
- 45. Human Trafficking Prohibition.** Under Section 2155.0061, Texas Government Code, Provider certifies that the entity named in this Contract is not ineligible to receive the specified contract and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.
- 46. COVID-19 Vaccination.** EVS certifies that, for so long as such a requirement is prohibited by applicable law, including without limitation Section 161.0085 of the Texas Government Code, it does not require its customers to provide any documentation certifying the customer's COVID-19 vaccination or post-transmission recovery on entry to, to gain access to, or to receive service from the EVS' business. EVS acknowledges that such a vaccine or recovery requirement would make EVS ineligible for a state-funded contract. This Section 46 shall not be construed to prohibit the activities described in Sections 161.0085(e)(1)-(2) of the Texas Health and Safety Code.
- 47. Foreign Ownership.** Pursuant to Government Code Section 2274.0102, EVS certifies that neither it nor its parent company, nor any affiliate of EVS or its parent company, is: (1) majority owned or controlled by citizens or governmental entities of China, Iran, North Korea, Russia, or any other country designated by the Governor of Texas under Government Code Section 2274.0103, or (2) headquartered in any of those countries.
- 48. Prohibited Boycotts.** If EVS is required to make a verification pursuant to Section 2274.002 of the Texas Government Code, EVS verifies that EVS does not boycott energy companies and will not boycott energy companies during the term of the Contract. If EVS does not make that verification, EVS must notify the Agency and state why the verification is not required.
- 49. Firearm Entities.** If EVS is required to make a verification pursuant to Section 2274.002 of the Texas Government Code, EVS verifies that it (1) does not have a practice, policy, guidance, or directive that discriminates against a "firearm entity" or "firearm trade association" as those terms are defined in Texas Government Code section 2274.001 and (2) will not discriminate during the term of the Contract against a firearm entity or firearm trade association. If EVS does not make that verification, EVS must notify the GLO and state why the verification is not required.
- 50. 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, which such consent shall not be unreasonably withheld, delayed or denied. This Agreement shall be freely assignable by EVS to another entity within its family of companies, or to another entity with common ownership and control as that of EVS or is controlled by EVS. In all other cases EVS may not assign or transfer the Agreement without Company's prior written consent, which shall not be unreasonably withheld, delayed or denied, or frustrate EVS's obligations as a publicly traded company. Such assignments 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.
- 51. NOTICES.** Every notice required under this Agreement may be (i) sent by electronic delivery to the applicable email address below; (ii) mailed first class postage prepaid or by other courier or delivery service to the applicable address below; or (iii) sent through other electronic means, including but not limited to, through Company's online or integrated access to the Service. Every notice shall be effective upon the following as applicable: (i) day of email sent; (ii) delivery by an overnight or other courier or delivery service, or three (3) days after pre-paid deposit with the postal service; or (iii) date of electronic notification through Company's online or integrated access to the Service. Company agrees that if it does not provide the notice information below, then EVS may use the address listed above to provide notice to Company. Either party may change its notice contact information upon notice to the other party.

	Company (To be filled in by Company)	EVS
E-mail Address	renee.vick@glo.texas.gov	evscontracts@equifax.com
Company Name	Texas General Land Office and Veterans Land Board	Equifax Workforce Solutions LLC
Company Street Address	1700 N. Congress Avenue	11432 Lackland Road
Company City, State, Zip Code	Austin, TX 78701	St. Louis, MO 63146
Attn: Company Notice Contact	Attn: Renee Vick	Attn: President

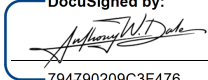
- 52. COUNTERPARTS/EXECUTION.** For the convenience of the parties, copies of this Agreement and Schedules hereof may be executed in two or more counterparts and signature pages exchanged by facsimile, email or other means of electronic transmission. The parties intend that counterpart copies signed 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.

[Signature page to follow]

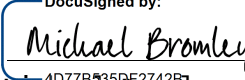
Company acknowledges receipt of Exhibit 1, "Notice to Users of Consumer Reports Obligations of Users Under the FCRA"; and Company represents that Company has read "Notice to Users of Consumer Reports Obligations of Users Under the FCRA" which explains Company's obligations under the FCRA as a user of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

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

**Texas General Land Office and Veterans Land Board**

By  
(signature):   
Name (print): Tony Dale  
Title: Executive Secretary  
Date: 5/11/2024

**Equifax Workforce Solutions LLC,  
provider of Equifax Verification Services**

By  
(signature):   
Name (print): Michael Bromley  
Title: SVP / GM Equifax Government Solutions  
Date: 5/11/2024

OGC 

DD 

DGC 

GC 

DLC 

**UNIVERSAL MEMBERSHIP AGREEMENT**  
**for**  
**Equifax Verification 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](http://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](http://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](http://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](http://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**  
**Equifax Verification Services**


**Exhibit 2**

**VERMONT FAIR CREDIT REPORTING CONTRACT CERTIFICATION**

The undersigned, Texas General Land Office and Veterans Land Board ("Company"), acknowledges that it subscribes to receive various information services from Equifax Workforce Solutions LLC, 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:** Texas General Land Office and Veterans Land Board

Signed By:   
794790209C3F476...

Printed Name and Title: Tony Dale, Executive Secretary

Account Number: \_\_\_\_\_

Date: 5/11/2024

**Please also include the following information:**

Compliance Officer or Person Responsible for Credit Reporting Compliance

Name: Kimilia Mangum

Title: Director of Land and Housing

Mailing Address: 1700 N. Congress Ave., Austin, TX 78701

E-Mail Address: kimilia.mangum@glo.texas.gov

Phone: 512-586-0233 Fax: 512-463-5698



**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 \*\*\*****COMPANY 06. OFFICE OF THE ATTORNEY GENERAL****SUB-COMPANY 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  
Equifax Verification Services****Exhibit 3**

*Para información en español, visite [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) o escribe a la Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.*

**A Summary of Your Rights Under the Fair Credit Reporting Act**

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 FCRA. **For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://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](http://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](http://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](http://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 (1-888-567-8688).

- The following FCRA right applies with respect to nationwide consumer reporting agencies:

**CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE**

**You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.** The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

- **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](http://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, N.W. Washington, DC 20552</p> <p>b. Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. 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 Financial Protection (OCFP) 1775 Duke Street Alexandria, VA 22314</p>
<p>3. Air carriers</p>	<p>Assistant General Counsel for Office of Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, S.E. Washington, DC 20590</p>
<p>4. Creditors Subject to the Surface Transportation Board</p>	<p>Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, S.W. Washington, DC 20423</p>
<p>5. Creditors Subject to the 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, S.W., Suite 8200 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>Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357</p>

## SECURITY EXHIBIT

This Security Exhibit (this “**Exhibit**”) describes the information security requirements applicable to Equifax Inc. (“**Equifax**”), on behalf of itself and its Affiliates, in connection with the agreement to which this Exhibit is attached (the “**Agreement**”) and the protection of Client’s or Company’s Personal Information which is disclosed in connection with the services provided by Equifax pursuant to the Agreement. For the purposes of this Exhibit, “**Affiliate**” shall mean Equifax Workforce Solutions LLC, provider of Equifax Verification Services (“**EVS**”), and “**Personal Information**” consists of personally identifiable information: (i) protected by privacy regulations in the United States applicable to Equifax’s provision of Services under the Universal Membership Agreement – Contract No. 24-134-000-E464 between the parties effective May 1, 2024 (the “**Agreement**”); and (ii) disclosed by Client to Equifax in connection with the Services provided pursuant to the Agreement including, but not limited to as applicable, customer names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. Terms that are capitalized but not defined in this Exhibit have the meaning given in the Agreement.

### 1. Equifax Information Security Program

Equifax maintains an information security program (the “**Program**”) that includes the requirements set forth herein. The Program is designed to protect the confidentiality, integrity, and availability of Personal Information. The Program is governed by the Equifax Information Security Policy (the “**Policy**”), which was developed in alignment with the National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity (“**NIST CSF**”) and includes safeguards to protect Personal Information. The Policy is reviewed on an annual basis.

The requirements for the Program include: (a) a Senior Information Security Officer responsible for implementing, maintaining, and monitoring the Program; (b) defined roles and responsibilities that are established, implemented, and communicated; (c) reporting to the Equifax Board of Directors on the adequacy of the Program; (d) a privacy program, including supporting policies and procedures that are defined, documented, implemented, and continually updated with privacy roles and responsibilities that are established and communicated; and (e) assessment of the Program at planned intervals.

### 2. Incident Response and Notification

Equifax maintains processes and requirements for: (a) reporting of security incidents or potential security incidents by Equifax personnel; (b) classifying and triaging security incidents to determine urgency; (c) investigating and diagnosing security incidents; and (d) resolving and mitigating the impact of security incidents.

Except to the extent prohibited by law or law enforcement, Equifax will promptly notify Client following any confirmed material breach or compromise of the security, confidentiality, or integrity, of Personal Information contained in Equifax’s databases of client data, which compromise Equifax could reasonably expect to adversely impact Client through increased risk of fraud or consumer identity theft (“**Security Incident**”). Notwithstanding the foregoing, Equifax shall not be required to provide any notification or information that could be considered material, nonpublic information as defined in the Securities Exchange Act of 1934 or any other applicable law, rule, or regulation or any notification with respect to information contained in Equifax’s credit reporting databases that is not Personal Information or any other Equifax confidential information. Equifax will take reasonable actions to help prevent a recurrence of a Security Incident.

### 3. Access Controls

Equifax has processes in place designed to limit access to Equifax assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions. The processes include management of: (a) identities and credentials for authorized devices and users; (b) physical access to Equifax assets and facilities; (c) remote access; (d) access permissions based on principles of least privilege and separation of duties; (e) network integrity, incorporating network segregation where appropriate; and (f) authentications (e.g. single-factor, multi-factor) commensurate with the risk of the transaction.

With respect to Personal Information, Equifax shall:

- (a) confirm access assigned on a least-privileged basis and uses role-based access rights when available;
- (b) remove access from employees who no longer require access;
- (c) require employees to use unique user accounts which are not shared and passwords which meet the commercial standard practice for complexity and length;
- (d) require that two-factor authentication is in place when accessing Personal Information;
- (e) review access periodically to confirm that the above processes are operating effectively;

- (f) permit access only through Equifax authorized devices; and
- (g) require two-factor authentication where remote access is required for systems which process Personal Information. Only approved corporate remote access solutions will be used and such solutions shall confirm that access is protected by strong encryption consistent with commercial standards.

#### 4. Physical Security

Equifax maintains a policy with respect to physical security which implements and maintains security and safety safeguards to protect Personal Information and is designed to comply or align with applicable laws, regulations, contractual commitments, and industry standards relating to physical security and safety. All sites where Personal Information is processed or stored have implemented physical security requirements that include physical access control restrictions, visitor access requirements, and CCTV coverage of entrances and exits to support investigation of physical security incidents.

#### 5. Secure Configuration Management

Equifax maintains a layered series of technical security controls designed to prevent unauthorized access to Personal Information and to preserve the confidentiality, integrity, and availability of Personal Information. These controls include:

- (a) a software development lifecycle program that covers the inclusion of formal security requirements and the testing of security functionality before code is released into the production environment;
- (b) a vulnerability scanning program for infrastructure which is used to store and process Personal Information and third party annual penetration testing of applications used to store and process Personal Information;
- (c) restrictions on the storage and transfer of Personal Information on removable media such as USB devices, CDs or DVDs applying technical patterns of activity and generating alerts based on identified events;
- (d) clear responsibility for monitoring the immediately foregoing systems and responding to alerts;
- (e) maintenance of a process which establishes network time protocol syncing for infrastructure supporting the processing or storage of Personal Information;
- (f) change of vendor default passwords prior to the implementation of new equipment or software;
- (g) restricted access to certain Internet sites and applications by Equifax's employees, including preventing access to file sharing websites and webmail; and
- (h) implementation of web application firewalls for all external facing applications.

Equifax's configuration management technical requirements also require that Equifax: (a) deploy systems into its environment in accordance with established baseline configurations; (b) monitor for changes to configuration settings within Equifax systems; (c) restrict the ability to install software to authorized individuals; and (d) update established baseline configurations to reflect changes in requirements on a periodic basis.

#### 6. Data Classification, Handling, and Encryption

Equifax maintains a robust data classification, handling, and encryption framework. This framework is aligned to the NIST CSF.

#### 7. Vulnerability Management

The Policy requires the implementation of a vulnerability management plan which requires Equifax to: (a) monitor vulnerability information to determine applicability and potential impact to Equifax assets; (b) maintain a process to report identified vulnerabilities; (c) scan external and internal systems to identify vulnerabilities; (d) perform periodic penetration tests against externally-facing applications; (e) rank, prioritize and remediate identified vulnerabilities; and (f) have application and system owners mitigate vulnerabilities within established service level agreements (SLAs).

Equifax will utilize anti-malware software on workstations with access to Personal Information and on Windows servers that are used to process or store Personal Information. Virus definitions are updated on at least a daily basis. Equifax will maintain a software patching process that includes testing, change management processes, and installation of software patches and updates based on the criticality of the security vulnerability that the patch addresses.

#### 8. Information Systems and Assets Monitoring

The Policy requires that information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures, including the following: (a) establishing roles and responsibilities for monitoring security events and responding to detected threat activity; (b) implementing technologies and processes designed to detect and remediate operational issues with security detection tools; (c) monitoring networks, applications, and endpoints to detect threat activity; (d) maintaining a logging and alerting infrastructure to collect audit logs and monitor audit logs for evidence of threat activity; (e) using a security event and incident management system to analyze audit logs and detect threat activity; and (f) testing the efficacy of fraud monitoring tools on a periodic basis and remediating identified issues.

#### 9. Asset Management

Equifax specifies how individuals within Equifax IT identify, classify, and track hardware, software and data assets through their lifecycle from acquisition planning to disposal, while reducing risk. This includes the following: (a) review of IT asset information with respect to financial, physical (location), and security information related to a given asset; (b) tracking and protection of IT assets that support the business processes they enable; and (c) requiring users of IT assets to follow appropriate administrative, technical, and physical information safeguards to protect IT assets. Equifax's IT asset management strategy is also governed by Equifax's asset management technical requirements, which require that Equifax maintain an inventory of assets and require that assets are securely disposed of when no longer required.

#### 10. Personnel Security

Equifax maintains a process for recruiting, onboarding, and managing employees that includes the following security requirements: (a) pre-employment screening for all employees with access to Personal Information or to sites that process or store Personal Information; (b) a security awareness program, completed at least annually, to increase and maintain employee awareness of security risks and of the requirements of their role in protecting Personal Information; and (c) completion of additional security awareness training based on job role and access.

#### 11. Third Party Oversight

Equifax has a team that is responsible for oversight and monitoring of third parties. Third parties are required to adhere to security requirements for maintaining appropriate administrative, technical, and physical information safeguards to protect Personal Information. Third parties are required to comply with applicable laws, regulations, industry standards, and contractual commitments relating to information security.

Equifax conducts appropriate due diligence and risk assessments before entering into a contract with a third party. The extensiveness of the due diligence process is determined by the third party's risk category. The results of such due diligence are used by Equifax to evaluate and assess, in part, the risk exposure the third party presents to Equifax. Equifax performs oversight and ongoing monitoring of third parties to evaluate their compliance with Equifax security requirements. The risk category of each third party determines the frequency and scope of the ongoing monitoring and assessment of the third party's compliance program. Equifax will take prompt action to address relevant compliance matters identified through the monitoring process, which could include suspending or terminating the third party relationship when appropriate.

## 12. Business Continuity and Disaster Recovery

Equifax maintains a comprehensive business continuity and disaster recovery framework that is reviewed and approved by relevant company management on a periodic basis. The requirements of the framework are defined by Equifax's Business Continuity and Disaster Recovery Technical Requirements, which require Equifax to do the following:

- (a) execute contingency plans, including business continuity and disaster recovery, during or after an event as deemed necessary for plan activation;
- (b) update contingency plans on a periodic basis, as a result of an incident/event, or based on the results of a contingency plan test;
- (c) test contingency plans on a periodic basis;
- (d) use alternate sites to permit the transfer and resumption of critical information systems and processes when the primary site capabilities are unavailable;
- (e) complete secure backups of information systems and data; and
- (f) perform testing of the integrity of backups on select applications on a periodic basis.

13. Assessment. Company may, upon request, conduct a security assessment ("Assessment") in order to examine EVS's performance of this Agreement. An Assessment will be conducted (i) during regular business hours, (ii) at Company's sole expense, (iii) no more frequently than once per calendar year, (iv) on a mutually agreed upon date but no less than thirty (30) days advance notice, and (v) subject to EVS' security policies over its facilities and systems. The right to conduct an Assessment does not allow Company to perform security testing, vulnerability assessment, or penetration testing against EVS. EVS will not be required to provide access to the proprietary data of EVS or of its other clients. All information learned or exchanged in connection with an Assessment shall be kept confidential. An Assessment shall be defined as the Company having the right to:

- 1. review the executive summary of third party audit report (e.g. SOC 2 Type 2 report or equivalent);
- 2. review EVS's Information Security Policy, End User Information Security Policy, Corporate Security Policy, and External Party Information Security Policy (collectively, "Policies"), within an EVS office. Alternatively, and upon request, Company may view the Policies, subject to EVS security and confidentiality requirements, via an online presentation hosted by EVS;
- 3. review high level network and infrastructure diagrams; and
- 4. participate in a "Question and Answer" session with subject matter experts.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



SCHEDULE A  
TO THE UNIVERSAL MEMBERSHIP AGREEMENT  
EQUIFAX VERIFICATION SERVICES FOR MORTGAGE & HOUSING

“Company” or “GLO”:	Texas General Land Office and Veterans Land Board
“Effective Date” of this Schedule A:	May 1, 2024
Industry Type:	Mortgage & Housing
“Agreement”:	Universal Membership Agreement – Contract # 24-134-000-E464
Agreement effective date:	May 1, 2024

Company may request various Services from EVS (i) during the Term of this Schedule A, (ii) in accordance with the Agreement and this Schedule A (which is part of the Agreement), and (iii) only when intended to be used for the use cases described below. EVS shall provide the Services in accordance with the Agreement. The Services are described in Schedule A-1. Some Services have additional terms and conditions which are referenced in Schedule A-2. Company will pay EVS for the Services pursuant to the terms of Schedule A-3. Unless otherwise provided, all defined terms used herein shall have the meaning ascribed to them in the Agreement. To the extent Sections 4, 7, 9, and 11-51 of the UMA conflict with this Schedule A, such identified sections of the UMA shall govern and control.

This Schedule A specifically supersedes and replaces any Schedules, Exhibits, Statements of Work, and other product or pricing agreements between the parties that predate this Schedule A and which relate to the Service(s) as provided in this Schedule A. It is noted that even if the prior agreements contain an “entire agreement” or “merger” clause, any such Schedules, Statements of Work, and/or other product or pricing agreements are terminated, but only to the extent as relevant to the Services described in this Schedule. For the avoidance of doubt, the parties agree that upon execution of this Schedule A effective May 1, 2024, the Schedule A effective as of May 1, 2021, and as amended, between Texas General Land Office and Veterans Land Board and TALX Corporation shall be terminated and of no further force or effect.

This Schedule A shall be for an initial term of one (1) year (the “Initial Term”), effective as of the Effective Date of May 1, 2024 to April 30, 2025, and may be extended for three (3) discrete annual terms (“Renewal Term(s)”), with pricing reflected in Schedule A-3, to be negotiated and mutually agreed upon each year to the next, given the Company’s budget authority. Renewal Terms must be requested by Company at least thirty (30) days in advance of the then-applicable expiration date. In no event will this Schedule A remain in effect after April 30, 2028.

1. **Company Information.** *(Please use the physical business location address; a P.O. Box is not acceptable.)*

Company Name:	Texas General Land Office	Phone:	512-463-5001
Address:	1700 N. Congress Ave.	State:	TX
City:	Austin	Zip Code:	78701

2. **Main Contact Information.**

Name:	Renee Vick	Phone:	512-463-5044
Title:	Staff Services Officer	Email:	renee.vick@glo.texas.gov

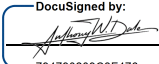
[Signature page to follow]

**IN WITNESS WHEREOF**, the parties have duly executed this Schedule A (including all attachments hereto) on the last date indicated below.

**Texas General Land Office and Veterans Land Board**

By: 

DocuSigned by:



794790209C3F476...

Name (print): Tony Dale

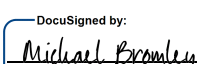
Title: Executive Secretary

Date: 5/11/2024

**Equifax Workforce Solutions LLC, provider of Equifax Verification Services**

By: 

DocuSigned by:



4D77B535DF2742B...

Name (print): Michael Bromley

Title: SVP / GM Equifax Government Solut

Date: 5/11/2024

**SCHEDULE A-1****SERVICE DESCRIPTIONS****I. THE WORK NUMBER® SERVICES.**

**A. The Work Number Verification of Employment (“Employment Verification” or “VOE”).** An Employment Verification includes, where available, 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. Employment Verifications obtained may provide Data from current employers and/or previous employers.

- (1) **VOE – Mortgage (“Mortgage VOE”).** Mortgage VOE instantly delivers the VOE service, with all available records during the past thirty-six (36) months from the date of the request.
- (2) **VOE – Mortgage (“Mortgage VOE with Receipt”).** Mortgage VOE with Receipt instantly delivers the Mortgage VOE service, with the ability to print a receipt for each Transaction.
- (3) **VOE – Employment Select (“Employment Select VOE”).** Employment Select VOE instantly delivers the VOE service, with only those available records having an Active employment status during the past sixty (60) days from the date of the request.
- (4) **VOE - Employment Select+™ (“Employment Select+ VOE”).** Employment Select+ VOE instantly delivers the VOE service, with all available records during the past thirty-five (35) days from the date of the request.
- (5) **VOE - Mortgage Select All™ (“Mortgage Select All VOE”).** Mortgage Select All VOE instantly delivers the VOE service, with all available records.
- (6) **VOE – All Employers Within 60 Months™ (“Mortgage VOE 60”).** Mortgage VOE 60 instantly delivers the VOE service, with all available records during the past sixty (60) months from the date of the request.
- (7) **VOE – All Employers Within 36 Months™ (“Mortgage VOE 36”).** Mortgage VOE 36 instantly delivers the VOE service, with all available records during the past thirty-six (36) months from the date of the request.
- (8) **VOE – All Employers Within 24 Months™ (“Mortgage VOE 24”).** Mortgage VOE 24 instantly delivers the VOE service, with all available records during the past twenty-four (24) months from the date of the request.
- (9) **VOE – All Employers Within 12 Months™ (“Mortgage VOE 12”).** Mortgage VOE 12 instantly delivers the VOE service, with all available records during the past twelve (12) months from the date of the request.
- (10) **VOE – Mortgage Employer Select (“Mortgage Employer Select VOE”).** Mortgage Employer Select VOE delivers a preview of all available employment records from current employers and/or previous employers. One or more employment records may be selected from the preview, after which Mortgage Employer Select VOE instantly delivers the VOE service on the requested records. At least one selection on the preview is required in order to receive the VOE service.

**B. The Work Number Verification of Income (“Income Verification” or “VOI”).** An Income Verification includes, where available, the Data provided in a VOE, plus the current year-to-date pay plus the most recent two (2) years of payroll Data. Income Verifications obtained may provide Data from current employers and/or previous employers.

- (1) **VOI – Mortgage (“Mortgage VOI”).** Mortgage VOI instantly delivers the VOI service, with all available records during the past thirty-six (36) months from the date of the request.
- (2) **VOI – Mortgage (“Mortgage VOI with Receipt”).** Mortgage VOI with Receipt instantly delivers the Mortgage VOI service, with the ability to print a receipt for each Transaction.
- (3) **VOI - Mortgage Select All™ (“Mortgage Select All VOI”).** Mortgage Select All VOI instantly delivers the VOI service, with all available records.
- (4) **VOI – All Employers Within 60 Months™ (“Mortgage VOI 60”).** Mortgage VOI 60 instantly delivers the VOI service, with all available records during the past sixty (60) months from the date of the request.
- (5) **VOI – All Employers Within 36 Months™ (“Mortgage VOI 36”).** Mortgage VOI 36 instantly delivers the VOI service, with all available records during the past thirty-six (36) months from the date of the request.
- (6) **VOI – All Employers Within 24 Months™ (“Mortgage VOI 24”).** Mortgage VOI 24 instantly delivers the VOI service, with all available records during the past twenty-four (24) months from the date of the request.
- (7) **VOI – All Employers Within 12 Months™ (“Mortgage VOI 12”).** Mortgage VOI 12 instantly delivers the VOI service, with all available records during the past twelve (12) months from the date of the request.

- (8) **VOI – Mortgage Ultimate™ (“Mortgage VOI Ultimate”).** Mortgage VOI Ultimate instantly delivers the VOI service, with only those available records having an Active employment status during the past ninety (90) days and only those available records having an employment status from current and previous employers during the past twenty-four (24) months from the date of the request. As a part of Mortgage VOI Ultimate, Company may obtain up to three (3) additional Income or Employment Verifications with the same parameters as applied to the original request for such Consumer within a ninety (90) day period from the date of the original Mortgage VOI Ultimate request.
- (9) **VOI – Mortgage Employer Select (“Mortgage Employer Select VOI”).** Mortgage Employer Select VOI delivers a preview of all available employment records from current employers and/or previous employers. One or more employment records may be selected from the preview, after which Mortgage Employer Select VOI instantly delivers the VOI service on the requested records. At least one selection on the preview is required in order to receive the VOI service.
- C. **eBatch VOE.** eBatch VOE delivers a VOE in a batch delivery mode for the selected employment status available.
- D. **eBatch VOI.** eBatch VOI delivers a VOI in a batch delivery mode for the selected employment status available.
- E. **Point-in-Time™ Verification (“Point-in-Time”).** Point-in-Time provides an Income Verification from a specific point in time using a historical date, which may not be earlier than 2006, requested by the Company.
- F. **Portfolio Review – Employment Monitoring.** Portfolio Review – Employment Monitoring allows Company to monitor a portfolio of Consumer accounts. At least once during each twelve (12) month period that Company receives the service, Company must submit a portfolio of Consumer accounts to EVS and EVS will return initial matches from The Work Number® database for the submitted Consumers to establish an information baseline consisting of the data elements described below (“Baseline File”). Once the Baseline File has been processed, Company may choose to monitor the employment status for each Consumer in the Baseline File. Company may choose the date(s) in which it receives such monitoring by completing The Work Number Portfolio Review Configuration Checklist and submitting it to EVS in writing prior to implementation. EVS will return to Company changes to the employment status for each account in the Company’s portfolio as appropriate. Company may add new accounts or retire existing accounts from Company’s portfolio by submitting a file in the required format, and as to each new account added, EVS will provide an information baseline and monitoring thereafter. EVS will perform this monitoring service for a period of up to twelve (12) months from receipt of the portfolio. Company must then submit a new portfolio of Consumer accounts for each additional twelve (12) month period it wishes to monitor. The Portfolio Review – Employment Monitoring Service, provided in a batch-only delivery mode, includes, where available, the Consumer’s (i) name, (ii) employment status, (iii) social security number, and (iv) information current as of date. Company will request the Portfolio Review – Employment Monitoring service via the eBatch Service website. EVS will post a return file via a secure batch website. The Baseline File will contain the full Portfolio Review – Employment service. Subsequent notification files for the employment status will contain the inclusion reason for the changed account(s), along with the data elements provided in the baseline for such account(s). EVS will monitor changes in employment status.
- G. **Portfolio Review – Employment.** Portfolio Review – Employment, provided in a eBatch-only delivery mode, includes, where available, the Consumer’s (i) name, (ii) employment status, (iii) social security number, and (iv) information current as of date. Company will request the Portfolio Review - Employment Service via the eBatch Service website.
- H. **Portfolio Review – Income Monitoring.** Portfolio Review – Income Monitoring allows Company to monitor a portfolio of Consumer accounts. At least once during each twelve (12) month period that Company receives the service, Company must submit a portfolio of Consumer accounts to EVS and EVS will return initial matches from The Work Number® database for the submitted Consumers to establish an information baseline consisting of the data elements described below (“Baseline File”). Once the Baseline File has been processed, Company may choose to monitor the employment status and rate of pay for each Consumer in the Baseline File. Company may choose the date(s) in which it receives such monitoring by completing The Work Number Portfolio Review Configuration Checklist and submitting it to EVS in writing prior to implementation. EVS will return to Company changes to the employment status and rate of pay fields for each account in the Company’s portfolio as appropriate. Company may add new accounts or retire existing accounts from Company’s portfolio by submitting a file in the required format, and as to each new account added, EVS will provide an information baseline and monitoring thereafter. EVS will perform this monitoring service for a period of up to twelve (12) months from receipt of the portfolio. Company must then submit a new portfolio of Consumer accounts for each additional twelve (12) month period it wishes to monitor. The Portfolio Review – Income Service, provided in a batch-only delivery mode, includes where available, the Consumer’s (i) name, (ii) employment status, (iii) social security number, (iv) pay frequency, (v) current year annualized income, (vi) rate of pay, and (vii) information current as of date. Company will request the Portfolio Review – Income Monitoring Service via the eBatch Service websites. EVS will post a return file via a secure batch website. The Baseline File will contain the full Portfolio Review – Income Service. Subsequent notification files for the monitored data fields will contain the inclusion reason for the changed account(s), along with the data elements provided in the baseline for such account(s). EVS will monitor changes in employment status, as well as +/- 10% change in Rate of Pay.

- I. **Portfolio Review – Income.** Portfolio Review – Income, provided in a ebatch-only delivery mode, includes, where available, the Consumer's (i) name, (ii) employment status, (iii) social security number, (iv) pay frequency, (v) current year annualized income, (vi) rate of pay, and (vii) information current as of date. Company will request the Portfolio Review – Income Service via the eBatch Service website.
- J. **Reverify Verification ("Reverify").** Each time EVS performs a verification, EVS assigns such verification a unique reference number. Using the reference number and the last four digits of an individual's social security number, Company may obtain an updated VOE on the original verification (VOE or VOI) performed on such individual, as long as such request is within one hundred twenty (120) days of the original verification performed. Reverify will only return Data that has been updated within the past thirty five (35) days of the request.
- K. **Audit by Loan Number ("ABLN") Program.** The ABLN Program allows Government Sponsored Entities ("GSE") to access copies of certain verifications through retrieval directly from EVS. Company grants authority for GSE to view copies of Employment, Employment with Income, and/or IRS Income Verifications originally requested by Company. Company agrees to provide EVS with the relevant unique identifier meaningful to GSE and Company ("Loan Number") within the appropriate required order field for its VOE, VOI, and/or IRS Tax Transcript Fulfillment. By providing the Loan Number, Company acknowledges and agrees that EVS may provide audit copies of verifications to GSE to more easily facilitate the sale of mortgage loans by Company to GSE. EVS shall provide GSE with the exact duplicate of the previous, original verification(s) for the specific Loan Number as requested by Company. Company will be charged directly for ABLN orders placed by GSE when the Loan Number indicates that the order is associated with the ABLN Program. Audit copies of the verifications will be available for up to one hundred and eighty (180) days after the original verification was completed; thereafter, a new verification must be completed by the lender for an audit copy to be available. The ABLN per SSN fee includes all audit copies of the Standard VOE, Standard VOI, Network VOE, Network VOI, and IRS Tax Transcript Fulfillment available for all social security numbers on the loan for a period of ninety (90) days. ABLN fees will reset every ninety (90) day period.
- L. **Included Services.** The following Service is also available for use with The Work Number Services. Company will be billed for this Service when a Transaction is completed for Company.
  - (1) **Audit-by-Reference Number ("ABRN").** Each time EVS performs a verification, EVS assigns such verification a unique reference number. Using the reference number and the last four digits of an individual's social security number (SSN), Company may obtain an ABRN copy as available by Service and selected by Company. The ABRN copy is an exact duplicate of the previous, original verification performed on such individual.

## 2. OTHER EVS SERVICES.

### A. Network Verification.

- (1) **Network Verification – Employment ("Network VOE").** Network VOE delivers detailed employment verifications for records not instantly available on The Work Number® Service. The report is consistent in Data elements and format to a VOE, except for Self-Employed VOE. EVS provides the Network VOE as a service provider on behalf of Company and not as a consumer reporting agency.
  - (a) **Self-Employed VOE.** Self-Employed VOE provides information obtained through external search source(s) that may help Company validate self-employed and tax-preparer information. Self-Employed VOE provides, where available, (i) Consumer's business/regulatory license, (ii) number of years the Consumer's company has been in business, (iii) percentage of the Consumer's ownership or partnership, (iv) Consumer's position title, and (v) if the Consumer's company is open and operational or closed.
  - (b) **Standard Network VOE.** Standard Network VOE provides a Network VOE to Company upon completion.
  - (c) **Standard Network VOE + RVOE (as described below).** Standard Network VOE + RVOE includes a Standard Network VOE plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOE order on the date of Company's choice, with the ability to modify that date after order submission.
  - d) **Priority Next Day™ VOE.** Priority Next Day VOE provides a Standard Network VOE by 11:59 PM CT on the next business day following Company's request.
  - e) **Priority Next Day VOE + RVOE.** Priority Next Day VOE + RVOE includes a Priority Next Day VOE plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOE order on the date of Company's choice, with the ability to modify that date after order submission.
  - f) **Priority Two Day™ VOE.** Priority Two Day VOE provides a Standard Network VOE by 11:59 PM CT on the second business day following Company's request.
  - g) **Priority Two Day VOE + RVOE.** Priority Two Day VOE + RVOE includes a Priority Two Day VOE plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOE order on the date of Company's choice, with the ability to modify that date after order submission.

- (2) **Network Verification – Income (“Network VOI”).** Network VOI delivers detailed employment and income verifications for records not instantly available on The Work Number® Service. The report is consistent in Data elements and format to a VOI. EVS provides the Network VOI as a service provider on behalf of Company and not as a consumer reporting agency.
- (a) **Standard Network VOI.** Standard Network VOI provides a Network VOI to Company upon completion.
  - (b) **Standard Network VOI + RVOE.** Standard Network VOI + RVOE includes a Network VOI plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOI order on the date of Company’s choice, with the ability to modify that date after order submission.
  - (c) **Priority Next Day™ VOI.** Priority Next Day VOI provides a Standard Network VOI by 11:59 PM CT on the next business day following Company’s request.
  - (d) **Priority Next Day VOI + RVOE.** Priority Next Day VOI + RVOE includes a Priority Next Day VOI plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOI order on the date of Company’s choice, with the ability to modify that date after order submission.
  - (e) **Priority Two Day™ VOI.** Priority Two Day VOI provides a Standard Network VOI by 11:59 PM CT on the second business day following Company’s request.
  - (f) **Priority Two Day VOI + RVOE.** Priority Two Day VOI + RVOE includes a Priority Two Day VOI plus the RVOE service. The RVOE service will automatically order an updated verification for the original Standard Network VOI order on the date of Company’s choice, with the ability to modify that date after order submission.
- (3) **Network Verification Reverify (“RVOE”).** Each time EVS performs a Network VOE/VOI, EVS assigns such verification a unique reference number. Using the reference number and the last four digits of an individual’s social security number, Company may obtain updated employment data on the original verification (Network VOE/VOI) performed on such individual, as long as such request is within one hundred twenty (120) days of the original verification performed. EVS will contact the employer to confirm all employment-related data, which includes: employer name, job title, start date, and employment status.

#### **B. IRS Income Verification Services.**

- (1) **IRS Tax Transcript Fulfillment.** EVS shall provide Company with the IRS Tax Transcript Fulfillment Service as requested by Company. Tax documents may be ordered by a representative of Company. A valid completed IRS consent form (such as IRS Form 4506-C), which has been signed by the Consumer within the timeframe allowed by the Internal Revenue Service (“IRS”) prior to submission, is required for every order. EVS shall perform an initial quality review of IRS consent forms submitted by a representative of Company to ensure that the appropriate consumer information and signature are provided to EVS prior to the delivery to the IRS. The tax transcript document provided to EVS by the IRS is then made available to Company. EVS shall provide Company with the Tax Transcript Summary Report when available. This report provides an overview of key data elements and analysis from each tax transcript ordered by Company.

#### **C. Social Security Verification Services.**

- (1) **SSA Authentication Report.** A representative of Company may submit a name, date of birth, and social security number for validation that the name, submitted SSN, and date of birth match the information on the Social Security Administration (“SSA”) database. A valid completed SSA-89 consent or other form of consent deemed appropriate by the SSA, which has been signed by the Consumer within the timeframe allowed by the SSA prior to submission, is required for processing of every order. EVS shall perform an initial quality review of SSA consent forms submitted by a representative of Company to ensure that the appropriate Consumer information and signature are provided to EVS prior to fulfillment with the SSA.
- (2) **Identity Usage and Address History Report.** A representative of Company may submit a social security number (SSN) to determine if the SSN is valid; where and when the SSN was issued; previous addresses; additional SSNs associated with the Consumer; and/or if multiple identities are associated with the SSN. This proprietary search and comparison process produces a comprehensive report that is made available to the Company.
- (3) **SSA Death Master File Audit.** EVS will screen the social security number (SSN) of the Consumer against the SSA Death Master File to ensure the SSN provided by the Consumer has not been associated to a deceased individual. If the SSN has been reported as associated with a deceased individual the name, date of death, and place of record for the deceased individual will be reported.

**SCHEDULE A-2****ADDITIONAL TERMS AND CONDITIONS****1. TERMS AND CONDITIONS APPLICABLE TO ALL SERVICES.**

- A. Use.** Data provided from The Work Number is limited to a single use for the permissible purpose in which it was obtained. Information provided from other EVS Services is limited to a single use for the purpose in which it was obtained.
- B. "Transaction"** means a database search that returns Data or Information as requested by Company, unless otherwise defined.
- C. Delivery.** The Services will provide automated or manual access to requested Data and/or Information, as available by Service and selected by Company, (i) instantly via the internet ("Web"), (ii) instantly via system-to-system integration ("Integrated"), or (iii) via a batch-only delivery mode ("eBatch"). Data and/or Information will be delivered via the same mode it was requested.
- D. Audit.** Upon request by EVS at any time, Company shall provide Consumer authorizations to verify the Consumer's information, including but not limited to the Consumer's income, and Company shall provide EVS with records as EVS may reasonably request to conduct such audit(s). Company's failure to fully cooperate or to produce requested Consumer authorizations may result in immediate suspension of the Services until such time as Company corrects any discrepancy revealed by such audit.
- E. Modification of Service.** EVS may modify any of the Service Descriptions set forth in Schedule A on thirty (30) days' notice to Company. Company may terminate the Service within thirty (30) days after notice of a modification to the Service Description on written notice to EVS. Absence of such termination shall constitute Company's agreement to the modification.
- F. Compliance with Laws.** Company will comply with all applicable laws, statutes and regulations regarding the Services including, but not limited to, the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA"). Where applicable, Company will comply with Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq. ("GLBA") and the implementing regulations issued thereunder and any other applicable statutes or federal laws, Company will not use or disclose any Information other than in accordance with Section 6802(c) or with one of the General Exceptions of Section 6802(e) of the GLBA and applicable regulations and all other US privacy laws.

**2. TERMS AND CONDITIONS APPLICABLE TO THE WORK NUMBER® SERVICES.**

- A. FCRA.** THE PARTIES ACKNOWLEDGE THAT THE WORK NUMBER SERVICES LISTED IN THIS SECTION ARE A "CONSUMER REPORT" AS DEFINED BY THE FCRA.
- B. Input Requirements.** Company may obtain The Work Number Services by providing a Consumer's social security number. Company represents that it has authorization from the Consumer authorizing Company to verify income data. Company need not use any particular form of authorization to verify the Consumer's income, provided the authorization is auditable and demonstrates to a reasonable degree of certainty that the Consumer has authorized Company to receive the income Data. Additionally, if ordering a service that is provided in a batch delivery mode, Company is required to periodically create and deliver a request file of Consumer social security numbers to EVS. EVS will process the request file and deliver a return file of results on social security numbers for which it has Data. Each party will bear the cost of producing their batch files. Upon submission of a file, Company is obligated to pay all charges and/or fees in accordance with the Agreement between EVS and Company. Company is responsible for providing a file in the correct format and for ensuring that the file being submitted is not in error. For eBatch VOE/VOI, Company will request the service on a minimum of one-hundred (100) Consumers per request.
- C. Active.** Data for which the Consumer's status field is populated as active by the employer, indicating that the Consumer is currently employed by that employer, shall be deemed to be "Active."
- D. Mortgage Employer Select VOE/VOI.** Mortgage Employer Select VOE and Mortgage Employer Select VOI will provide Company with a preview of all available employment records from current employers and/or previous employers, organized by employer name. Mortgage Employer Select VOE and Mortgage Employer Select VOI require Company to select one or more employment records from the preview in order to receive an employment and/or income verification. Mortgage Employer Select VOE and Mortgage Employer Select VOI will bill Company separately for (i) the preview and (ii) each record selected by Company from the preview and verified by the Service. Company will be billed for the preview whether or not Company selects any records. Previews are not required to display in "Order History."
- E. Point-in-Time.** Company will receive notification when a verification has been completed. Company acknowledges that Point-in-Time reports may be dependent upon response times by individual employers and may take up to five (5) days to complete. EVS will bill Company for all requests submitted, regardless if the request successfully returns data.
  - (1) Input Requirements.** Company may obtain a Point-in-Time report by providing (i) Consumer's social security number, (ii) Consumer's first and last name, (iii) Consumer's employer name, (iv) employer's full address, and (v) employer's phone number. Company must provide the original verification information being reviewed in addition to an authorization from the Consumer authorizing Company to verify income Data is required, provided the authorization is auditable and demonstrates to a reasonable degree of certainty that the Consumer has authorized Company to receive the income Data.
- F. Portfolio Review – Employment Monitoring/Income Monitoring.** The Monitoring Service requires that the Company periodically (at least once during each twelve (12) month period that Company receives the Service) create and deliver a request file of Consumer social security numbers to EVS. EVS will process the request file and deliver a return file of either Portfolio Review – Employment or Portfolio Review – Income for newly submitted Consumer social security numbers in order to create a baseline, or a monitoring file which consists of the Data elements available for monitoring as stated in the Portfolio Review – Employment Monitoring or Portfolio Review – Income Monitoring services (depending on the Service selected) for those social security numbers for which a baseline has been established on social security numbers for which it has Data. Each party will bear the cost of producing their batch files. Company shall advise EVS to terminate monitoring any account as to which Company does not have input requirements or as to which Company ceases to have permissible purpose or other requirements under FCRA.

**3. TERMS AND CONDITIONS APPLICABLE TO OTHER EVS SERVICES.**

- A. FCRA DISCLAIMER.** THE PARTIES ACKNOWLEDGE THAT THE OTHER EVS SERVICES ARE NOT CONSUMER REPORTS SUBJECT TO THE FCRA AND STATE LAW FCRA COUNTERPARTS. THE PARTIES ACKNOWLEDGE THAT THE PROVISIONS OF AND EXHIBITS TO THE AGREEMENT WHICH REQUIRE COMPLIANCE WITH FCRA STANDARDS SHALL NOT APPLY TO THESE SERVICES.
- B. CERTIFICATION.** COMPANY CERTIFIES THAT IT WILL NOT USE ANY INFORMATION OBTAINED FROM THE SERVICES LISTED IN THIS SECTION ("INFORMATION") IN SUCH A MANNER THAT CAUSES THE INFORMATION TO BE CHARACTERIZED AS A CONSUMER REPORT. COMPANY AND EVS AGREE THAT THE NON-FCRA VERIFICATION SERVICES PROVIDED HEREUNDER SHALL NOT CONSTITUTE A CONSUMER REPORT UNDER THE FCRA.
- C. Network Verification.** Company will receive notification when a verification has been completed. Company acknowledges that Network Verification Services are dependent upon response times by individual employers. EVS will bill Company for all requests submitted, regardless if the request successfully returns data, except as provided below in Section C(4).
- (1) Company Representation.** Company represents that EVS is authorized to obtain Data from third party providers acting as an agent on Company's behalf, and to make the limited agency known to such third party providers.
  - (2) Input Requirements.** Company may obtain a Network Verification by providing a (i) Consumer's social security number, (ii) Consumer's first and last name, (iii) Consumer's employer name, (iv) employer's full address, and (v) employer's phone number. For Network VOE, written authorization from the Consumer authorizing Company to verify employment Data may be required. For Network VOI, an authorization from the Consumer authorizing Company to verify income Data is required, provided the authorization is auditable and demonstrates to a reasonable degree of certainty that the Consumer has authorized Company to receive the income Data.
  - (3) Self-Employed VOE.** Company may obtain a Self-Employed VOE by providing a (i) Consumer's social security number, (ii) Consumer's first and last name, (iii) Consumer's business name, (iv) Consumer's full business address, (v) Consumer's business phone number, and (vi) Consumer's tax preparer information (first name and last name). If the tax preparer's information is not provided at order origination, EVS (i) will not provide parts (ii)-(v) listed above in the service description; (ii) will not validate the tax preparer information; and (iii) will only, where available, (a) validate the Consumer's business through external source search(es), and/or (b) obtain the Consumer's business/regulatory license from a regulatory source. For avoidance of doubt, whether or not Company includes tax preparer information, Company will be billed, regardless if the request successfully returns data.
  - (4) Priority Next Day™ VOE/VOI and Priority Two Day™ VOE/VOI.** EVS will not bill Company if EVS does not return data to Company within the designated time frame for Priority Next Day™ VOE/VOI or Priority Two Day™ VOE/VOI, unless Company opts to convert to the Standard Network VOE/VOI at order origination. If Company chooses to convert the Priority Next Day™ VOE/VOI or Priority Two Day™ VOE/VOI to a Standard Network VOE/VOI at order origination, the request will be billed at the Standard Network VOE/VOI price, regardless if the request successfully returns data.
  - (5) Automated RVOE Ordering Services.** The automated feature that orders the RVOE services is available only at order origination and only for certain services. Unless Company modifies the date, the order date for the RVOE service will default to thirty (30) days from the order origination date. The RVOE order date may be modified at any time up to two (2) days prior to the specified RVOE order date. The RVOE request will be automatically ordered on the default RVOE order date or the date Company specifies, either of which must be within a maximum of one hundred twenty (120) days from the order origination date. Unless otherwise noted here, requests will continue to follow existing processes to fulfill Network Verification orders.
- D. IRS Income Verification Services.**
- Company Certification.** Company certifies that Company has procedures and policies in place to validate the identities of all individuals authorized to submit and retrieve IRS transcripts on behalf of Company.
- E. Social Security Verification Services.**
- (1) Company Certification.** Company certifies that it will obtain the Social Security Verification Services solely for the purpose of identity verification and in connection with a credit transaction or other circumstance described in Section 604 of the FCRA, and not to determine a consumer's eligibility for credit, insurance, employment, or any other product or service and that Company will not use the verification service for any other purpose. Company certifies it will not use any Information in such a manner that causes the Information to be characterized as a "consumer report" as defined in the FCRA.
  - (2) SSA Authentication Report.** The SSA Authentication Report verifies whether a Consumer's social security number, name and date of birth match the Social Security Administration's ("SSA") Master File of SSN Holders and SSN Application System of Records ("SSA Records") for the specific purpose stated on the signed SSA-89 consent form or other written or electronic Consumer consent deemed appropriate by the SSA ("Consent").
- As a Financial Institution, as defined in the SSA Electronic Consent Based Social Security Number Verification Service ("eCBSV") User Agreement, Company agrees to abide by all terms, conditions, and requirements of the SSA eCBSV User Agreement. Company agrees to only submit SSA Authentication Report requests pursuant to Consumer Consent. Company agrees that it shall use the SSA Authentication Report results only for the purpose stated in the Consent, and shall make no further use or re-disclosure of the authentication. Company also acknowledges and agrees that any such further use or re-disclosure is subject to the penalties in Section 42 U.S.C § 1306(a)(1). Company agrees to produce supporting documentation upon request for purposes of compliance reviews and agrees to retain such documentation for a period of five (5) years from the date of the applicable SSA Authentication Report request. Supporting documentation must include evidence of the purpose and must be maintained in a way to clearly link the specific purpose of a transaction to the Consent and in a way that preserves the accuracy and integrity of the records and is accessible to the SSA and SSA's auditors. When storing these documents electronically, Company must destroy any original documents in paper form.



By submitting SSA Authentication Report requests to EVS, Company certifies that it has registered for using the eCBSV service and has submitted a Permitted Entity Certification to the SSA. Company acknowledges the requirement to submit a new Permitted Entity Certification every two years after the initial submission. Company certifies that it has provided consent for the SSA to access its Employer Identification Number ("EIN") and agrees to notify the SSA if Company's EIN changes. Company agrees to submit written notification to EVS and the SSA of any name change thirty (30) calendar days before submitting any requests for SSA Authentication Reports under the new name.

Company must not alter the Consent before or after the Consumer signs the Consent. If the Consumer later changes the period during which the Consent is valid, Company may not rely upon the Consent to request SSA Authentication Reports unless the Consumer annotated and initialed this change in the space provided on the Consent, including by a new electronic signature. Company must not rely on the Consent to submit an SSA Authentication Report request unless the request is submitted within the time specified on the Consent, either ninety (90) calendar days from the date the Consumer signs the Consent or by an alternate date established on the Consent. Consent may not be reused.

Company agrees that the SSA name, wording, and/or logo are confidential and will be protected in accordance with the confidentiality provisions of the Agreement. Company shall not utilize the SSA name, wording, and/or logo in any advertising or other marketing or promotional materials, nor shall Company advertise that Social Security Number Verifications provide or serve as identity verification.

Company understands the information received from records maintained by the SSA is protected by Federal statutes and regulations, including 5 U.S.C. §552a(i)(3) of the Privacy Act and 42 U.S.C. §1320b-10(a). Under these statutes, any person who knowingly and willfully requests or obtains any record concerning an individual from an Agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000. Also, SSA Authentication Report requests shall conform to Section 215, "Reducing Identity Fraud" of the Economic Growth, Regulatory Relief and Consumer Protection Act (42 U.S.C. §405(b)), as amended, and these requests must include the full name, date of birth, and SSN of each Consumer. With electronically signed Consent, Company acknowledges and agrees that it will obtain written consent electronically from the Consumer consistent with section 106 of the E-SIGN Act (15 U.S.C. §7006).

Company further understands that Company must properly safeguard any information that personally identifies a Consumer from loss, theft, or inadvertent disclosure, and in the event of loss, theft, or inadvertent disclosure, Company must immediately report such disclosure to EVS and must fully cooperate with EVS in providing any information required by the SSA. Company must put in place and follow adequate disaster recovery procedures.

In cases where the SSA authentication report results in a "no match", Company will take the following actions before making any referrals to SSA Field Offices to determine the nature of the problem: (1) determine whether the Data submitted for an SSA authentication report matches the data in the Company's records; and (2) if the data in the Company's records matches the Data submitted to SSA, then Company shall re-contact the individual who is the subject of the request to verify the original Data provided.

Company shall not transfer any personal information provided by EVS hereunder, including any authentication or non-authentication of name, date of birth or social security number ("Data") except to (i) the individual as to whom the authentication pertains or (ii) a party which has been granted authority to receive such information by the proper form, such as a completed SSA Direct Authorization form and which otherwise meets the requirements described herein ("Authorized End User").

Company shall require that an Authorized End User hereunder agree to the following as part of the agreement between Company and the Authorized End User. Each provision shall be in substantially the form contained in this Agreement, adjusted as appropriate for the change in parties.

- a) The Data Security provisions of the standard Agreement;
- b) The Confidentiality provisions of the standard Agreement;
- c) The Rights to Service provisions of the standard Agreement;
- d) The Service Description and Modification of Service provisions contained in this Schedule A.

Company understands that in order to ensure compliance with the terms of the Social Security Verification Service, the SSA may audit EVS's books and records associated with this Service. Company therefore agrees to cooperate and produce any documentation requested by EVS or the SSA to support such audit.

**SCHEDULE A-3****PAYMENT TERMS AND PRICING****1. PAYMENT TERMS AND CONDITIONS.**

- A. Invoices.** All Fees will be invoiced monthly. Invoices are due net thirty (30) days with interest accruing in accordance with Chapter 2251 of the Texas Government Code. Undisputed Invoices outstanding over forty-five (45) days will result in loss of access to the Service. Company will be invoiced electronically through Equifax's Electronic Invoice Presentation & Payment (EIPP) program. Requests for paper billing are available upon Company's request and are subject to additional monthly fees. Such fees are subject to modification by EVS at intervals of no less than one year, upon prior written notice. If payment is made by credit card, EVS will charge the credit card each month for Transactions completed in the prior month.

- (1) Billing Address.** *(If different from above, please enter the Company billing address to be included on the invoice; a P.O. Box is acceptable.)*

Attn:	Texas General Land Office - Renee Vick	Email:	vendorinvoices@glo.texas.gov
Address:	1700 N. Congress Ave.	State:	Austin
City:	Texas	Zip Code:	78701

- (2) Billing Contact.** *(If different from above, please enter the Company billing contact information.)*

Name:	Renee Vick	Phone:	512-463-5044
Title:	Staff Services Officer	Email:	renee.vick@glo.texas.gov

- (3) Invoice Disputes.** If Company, in good faith, disputes any portion of an amount invoiced, Company shall pay such amount as it in good faith believes to be correct, or undisputed, and provide notice in a detailed statement of the amount of the invoice which is disputed. All disputes must be submitted to EVS in accordance with Chapter 2251 of the Texas Government Code.

In the event that it is determined or agreed that Company must or will pay the disputed amount, then Company shall pay interest in accordance with Chapter 2251 of the Texas Government Code. In the event the Parties are unable to resolve such dispute, either party may pursue any remedy available at law or in equity to enforce its rights hereunder. For the avoidance of doubt, invoices issued which reflect a price change or pertain to fees for service modifications that have been accepted according to the terms of this Schedule, shall be deemed correct invoices for purposes of this section.

- B. Company Purchase Order.** If the use of a Purchase Order ("PO") or similar ordering document is required by Company, the following information must be provided as part of the Agreement. Failure to include this information reflects Company's agreement that a PO shall not be required by Company. Company shall provide notice of any PO changes no less than thirty (30) days prior to the expiration of the current PO. No additional terms and conditions shall be included in the PO unless expressly agreed to in writing by the Parties. If there is a conflict between language in the PO and the Agreement, the Agreement shall control. The PO Amount or dollar limit, if applicable, of initial PO does not limit or otherwise impact any minimum ordering obligations or purchase commitments specified herein. The PO effective dates (as defined below) does not impact the Effective Date(s) or Term(s) specified herein.

PO Number (or similar):	---	PO Amount:	---
PO Start Date:	---	PO End Date:	---
PO Contact Name:	---	PO Contact Email:	---

- C. Taxes.** Company (i) is tax exempt and has provided, or will provide, an exemption certificate, direct pay permit or other such appropriate documentation, prior to or no later than upon execution of the Agreement and this Schedule A, and (ii) shall not be charged taxes upon the provision of the Services provided Company retains its tax exempt status.

**2. SERVICE PRICING.** If not specifically stated herein, the price for each Service will be EVS's then-applicable standard price.

**A. Third Party Fees Applicable To All Services.**

- (1) Third Party Fee.** EVS will pass along any fees incurred by third parties to Company. EVS will post these third party fees as a separate line item on the invoices.
- (2) Technology Portal Delivery Fee.** EVS will pass along any delivery fees incurred for the use of a technology portal connection, as specified by Company, to Company. EVS will post these technology portal delivery fees as a separate line item on the invoices.

**B. The Work Number® Services.**

Select "Yes" or "No" for each Service	Service Name	Internal EFX Use	Use Case(s)	Price per Transaction				
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	Employment Verification Services							
	Mortgage VOE <sup>1</sup>	0210118655	<input checked="" type="checkbox"/> Origination <input checked="" type="checkbox"/> Reverification	\$35.00				
	Mortgage VOE with Receipt <sup>1</sup>	0210120258		\$71.50				
	Employment Select VOE	0210108396		\$90.95				
	Employment Select+ VOE	0210119394		\$96.95				
	Mortgage Select All VOE	0210115714		\$72.95				
	Mortgage VOE 60	0210115711		\$85.95				
	Mortgage VOE 36	0210115710		\$131.95				
	Mortgage VOE 24	0210115715		\$90.95				
	Mortgage VOE 12	0210115712		\$109.95				
		Mortgage Employer Select VOE <sup>2</sup>		0210122213		<table border="1"> <tr> <td>Preview</td> <td>Price per Record</td> </tr> <tr> <td>\$14.95</td> <td>\$61.50</td> </tr> </table>	Preview	Price per Record
Preview	Price per Record							
\$14.95	\$61.50							
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	Income Verification Services							
	Mortgage VOI <sup>1</sup>	0210118654	Origination	\$35.00				
	Mortgage VOI with Receipt <sup>1</sup>	0210120254		\$71.50				
	Mortgage Select All VOI	0210115714		\$72.95				
	Mortgage VOI 60	0210113104		\$85.95				
	Mortgage VOI 36	0210113087		\$131.95				
	Mortgage VOI 24	0210107886		\$90.95				
	Mortgage VOI 12	0210110603		\$109.95				
	Mortgage VOI Ultimate	0210108398		\$127.95				
		Mortgage Employer Select VOI <sup>2</sup>		0210122214	<table border="1"> <tr> <td>Preview</td> <td>Price per Record</td> </tr> <tr> <td>\$14.95</td> <td>\$61.50</td> </tr> </table>	Preview	Price per Record	\$14.95
Preview	Price per Record							
\$14.95	\$61.50							
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	eBatch VOE	0210110828	Reverification					
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	eBatch VOI	0210110827	<input type="checkbox"/> Origination <input type="checkbox"/> Reverification					
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Point-in-Time <sup>3</sup>							
	Point-in-Time – Employment	0210100054	Account Review	\$61.50				
	Point-in-Time – Income	0210100050						
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Portfolio Review – Employment Monitoring	0210111388						
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Portfolio Review – Employment	0210111388	Account Review					
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Portfolio Review – Income Monitoring	0210111387						
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Portfolio Review – Income	0210111387						
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	Reverify	0210100092	Reverification	Refer to Mortgage VOE for price. (\$35.00)				
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	ABLN Program							
	ABLN – Employment/Income	0210100832 3PF: 0210100838		\$0.00				
	ABLN – IRS Income (Only applies when the IRS Income Verification Services are selected below)	0227100839 3PF: 0227100693						
YES	ABRN	0210100002		\$4.50				

<sup>1</sup>Mortgage VOE, Mortgage VOE with Receipt, Mortgage VOI and Mortgage VOI with Receipt will bill a separate Transaction for different types of employer records returned. For example, if EVS returns records from both current and previous employers, EVS will bill two separate transactions, once for the current employer record and once for the previous employer record. With Mortgage VOE/VOI with Receipt, the receipt charge will only be billed once regardless of current and previous records returned.

<sup>2</sup>Mortgage Employer Select VOE and Mortgage Employer Select VOI will bill Company separately for (i) the preview and (ii) each record selected by Company from the preview and verified by the Service. Company will be billed for the preview whether or not Company selects any records.

<sup>3</sup>EVS will bill Company for all requests submitted, regardless if the request successfully returns data.

**C. Other EVS Services.**

Select "Yes" or "No" for each Service	Service Name	Internal EFX Use	Price per Transaction
<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	Network Verification		
	RVOE – Network Verification	0227100133	<i>Refer to Standard Network VOE for price.</i>
	Standard Network VOE <sup>4</sup>	0227100133 3PF: 0227103702	\$51.95
	Standard Network VOE + RVOE	0227117509	\$83.12
	Self-Employed VOE <sup>5</sup>	0210116024	\$62.35
	Priority Next Day™ VOE	0227115397	\$111.35
	Priority Next Day™ VOE + RVOE	0227117565	\$152.91
	Priority Two Day™ VOE	0227115396	\$88.25
	Priority Two Day™ VOE + RVOE	0227117564	\$129.81
	Standard Network VOI <sup>4</sup>	0227100059 3PF: 0227103702	\$51.95
	Standard Network VOI + RVOE	0227117509	\$83.12
	Priority Next Day™ VOI	0227118679	\$111.35
	Priority Next Day™ VOI + RVOE	0227118677	\$152.91
	Priority Two Day™ VOI	0227118675	\$88.25
	Priority Two Day™ VOI + RVOE	0227118676	\$129.81
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	IRS Income Verification Services		
	IRS Tax Transcript Fulfillment	0227110826 IRS: 0227100033	IRS Program Fee +\$8.00
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Social Security Verification Services		
	SSA Authentication Report <sup>5</sup>	0227100018 SSA: 0227100019	\$8.25
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	Identity Usage and Address History Report		<i>Included with SSA Authentication Report price</i>
<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	SSA Death Master File Audit		<i>Included with SSA Authentication Report price</i>

<sup>4</sup> EVS will bill Company for all requests submitted, regardless if the request successfully returns data.

<sup>5</sup> \$6.00 charge plus a \$2.25 processing fee.

**D. Additional Service Fees.**

	Internal EFX Use	
<b>Monthly Account Service Fee (ASF)</b> - This fee supports continual efforts by EVS which include, but are not limited to, maintaining The Work Number database; supporting data onboarding activities; and assisting with technical issues.	0210100693	\$100.00

**AMENDMENT TO THE UNIVERSAL MEMBERSHIP AGREEMENT**

This Amendment ("**Amendment**") is by and between Equifax Workforce Solutions LLC, a provider of Equifax Verification Services, ("**EVS**") and Texas General Land Office and Veterans Land Board ("**Customer**"), and is effective as of this **May 1, 2025** ("**Effective Date**"). This Amendment is entered into with the express agreement that except as addressed herein, all terms, conditions and stipulations contained in the Universal Membership Agreement between EVS and Customer, dated May 1, 2024, (as amended, the "**Agreement**") shall remain in full force and effect and without any change or modification whatsoever. For the purposes of this Amendment, all capitalized terms used herein and not otherwise defined shall have the meaning set forth in the Agreement.

**WHEREAS**, the parties desire to amend the Agreement, as set forth herein and hereby reaffirm and ratify each of the terms and conditions in the Agreement.

**NOW, THEREFORE**, in consideration of the premises and mutual covenants set forth herein, and for other valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree to amend the Agreement as follows:

1. **Amendment to Schedule A dated May 1, 2024.** The Third Paragraph of Schedule A is hereby deleted in its entirety and replaced as follows:

This Schedule A shall be for a term of one (1) year (the "First Renewal Term"), effective as of the Effective Date of May 1, 2025 to April 30, 2026, and may be extended for two (2) discrete annual terms ("Renewal Term(s)"), with pricing reflected in Schedule A-3, to be negotiated and mutually agreed upon each year to the next, given the Customer's budget authority. Renewal Terms must be requested by Customer at least thirty (30) days in advance of the then-applicable expiration date. In no event will this Schedule A remain in effect after April 30, 2028.

2. **Effect of Amendment: Entire Agreement.** This Amendment together with the Agreement (and any attachments, addenda, and supplements thereto) shall be the complete and exclusive statement of the Agreement between the parties as to the subject matter of the Agreement, and shall be binding upon each of the parties hereto, their respective successors and to the extent permitted their assigns. In the event of a conflict between the terms and conditions hereof, and the terms and conditions of the Agreement, the specific terms and conditions set forth in the Amendment shall govern. The parties agree that no term, condition, statement, or affirmation by either party beyond those specifically provided under this Agreement or Amendment - as may further be amended from time to time by consent of the parties - shall apply to the Agreement.

3. **Agency Purchase Orders** If the use of a Purchase Order ("**PO**") or similar ordering document is required by Customer, the following information must be provided as part of the Agreement. Failure to include this information reflects Customer's agreement that a PO shall not be required by Customer. Customer shall provide notice of any PO changes no less than thirty (30) days prior to the expiration of the current PO. No additional terms and conditions shall be included in the PO unless expressly agreed to in writing by the Parties. If there is a conflict between language in the PO and the Agreement, the Agreement shall control. The PO Amount or dollar limit, if applicable, of initial PO does not limit or otherwise impact any minimum ordering obligations or purchase commitments specified herein. The PO effective dates (as defined below) does not impact the Effective Date(s) or Term(s) specified herein.

PO Number (or similar):		PO Amount:	
PO Start Date:		PO End Date:	
PO Contact Name:		PO Contact Email:	

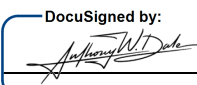
4. **Miscellaneous: Other Terms.** Unless otherwise permitted in the Agreement, neither this Amendment nor the Agreement can be amended or otherwise modified, except as agreed to in writing by each of the parties hereto.


This Amendment is accepted and agreed to by the following authorized representatives of the parties and each person signing below represents and warrants that he or she has the necessary authority to bind the principal set forth below.

IN WITNESS WHEREOF, the parties have executed this Amendment effective as of the Effective Date written above.

**Texas general Land Office and Veterans Land board**

**Equifax Workforce Solutions LLC**

By:   
Name: Tony Dale

By:   
Name: Michael Bromley

Title: Executive Secretary

Title: SVP, GM, Equifax Government Solutions

Date: 2/19/2025

Date: 2/19/2025

OGC  DD  DGC  GC 