MCDONALD'S OPERATOR
SOFTWARE AS A SERVICE AGREEMENT
FOR GUARDIAN ELECTRONIC I-9 AND E-VERIFY SERVICES

The terms of this **SUBSCRIPTION AND PROFESSIONAL SERVICES AGREEMENT** (this "**Agreement**") apply to and govern any Order, as defined below, entered into by and between Equifax Workforce Solutions LLC, having offices at 11432 Lackland Rd., St. Louis, MO 63146 ("**Provider**") and the entity or organization who has entered into the Order ("**Customer")**. The Parties may enter into one or more mutually executed ordering documents (each, an "**Order**") pursuant to which Customer may purchase or license the SaaS (referred to herein as the "**Services**").

WHEREAS, Customer is willing to enter into an agreement with Provider whereby Provider will provide and manage the hardware, software and connectivity which will enable Customer to electronically complete, store, and manage its I-9 and E-Verify records as required by U.S. employment eligibility verification rules.

NOW, THEREFORE, in consideration of the foregoing premises and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

DEFINITIONS.

"E-Verify" means the Internet-based employment eligibility verification system, operated by the U.S. Department of Homeland Security (DHS) in partnership with the Social Security Administration (SSA), which compares the information on an employee's Form I-9 with SSA and DHS records to verify the identity and employment eligibility of each newly hired employee and/or employee assigned to a covered federal contract.

"I-9" or "I-9 Record(s)" means the Form I-9 Employment Eligibility Verification Form which must be completed by employers for newly hired or re-hired employees, pursuant to the Immigration Reform and Control Act of 1986.

1. SaaS, Contractors/Consultants and Outsourcers and Upgrades.

A. SaaS. **"SaaS"** means collectively, access to and use of the proprietary Provider software **("Software")** which is accessed by having an identifying key for login via the internet, use of and access to any and all requisite software, hardware (which hardware may be modified, added to or replaced during the currency of this Agreement provided that the performance thereof is not caused to degrade), middle ware, hosting services, servers and the network comprising all or any of the following, namely, modems, leased circuits and other communications hardware and software (which network may be modified, added to or replaced during the currency of this Agreement provided that the performance thereof is not caused to fall materially below the said specifications) as the same operate together. Additional details defining the SaaS are provided on Exhibit A, attached hereto.

B. Contractors/Consultants and Outsourcers. Provider acknowledges that Customer enters into agreements with third parties to: (1) perform or manage Customer general IT services or significant IT projects, (2) to manage Customer's hardware and/or software; and/or (3) develop Customer's software applications ("**Contractors/Consultants"** and/or **"Outsourcers**"). Notwithstanding any contrary terms of this Agreement, Contractors/Consultants and Outsourcers shall be permitted to use the SaaS (a) solely for the benefit of Customer and (b) only in accordance with the terms of this Agreement.

C. Intentionally Deleted.

D. Upgrades. During the term of this Agreement, if Provider upgrades the version of the Software Customer is using, Customer will not be charged an upgrade fee. Should Provider offer additional optional software modules in the future that complement the Software, Customer may elect to purchase the optional software modules for an additional fee, however, Customer will have no obligation to do so.

2. Licenses.

A. Software*:* Subject to the terms of this Agreement, Provider hereby grants to Customer, its authorized users, and its Contractors/Consultant and Outsourcers a non-exclusive, world-wide, nontransferable, royalty free license to use the SaaS.

B. License Restrictions. Unless otherwise provided for in this Agreement, Customer may not, nor permit any third party to: (a) copy the Software; (b) modify, translate or otherwise create derivative works of the Software; (c) disassemble, decompile or reverse engineer the object code or source code of the Software; or (d) export or re-export the Software in violation of any United States export law or regulation.

3. Intellectual Property and Ownership.

A. Intellectual Property. The term "**Intellectual Property**" shall mean all ideas, concepts, know-how, documentation, techniques, data, reports, charts, graphs, works of authorship and improvements to the foregoing (whether or not patented or patentable, reduced to practice or included in the Provider's Confidential Information), and all other proprietary rights contributed to Provider or any of its employees (whether alone or jointly with others) at any time prior to the termination of this Agreement that result from the SaaS that Provider performs for Customer.

B. Ownership. All Intellectual Property is, shall be and shall remain the exclusive property of Provider. Notwithstanding the foregoing sentence, those work products which are fully customized, created, developed, and produced by Provider exclusively for Customer in connection with this Agreement which do not include products or materials that are derivatives of Provider's standard materials or Provider's proprietary information ("Customer Intellectual Property") shall be owned by Customer pursuant to the "work-made-for-hire" doctrine (rather than by assignment), as such term is defined in the 1976 Copyright Act. Customer Intellectual Property shall also include Customer Confidential Information. All Customer Intellectual Property shall be owned by Customer irrespective of any copyright notices or confidentiality legends to the contrary which may be placed on such works by Provider or by others. Provider waives all rights of "droit moral" or "moral rights of authors or creators" and/or any similar rights or principles of law which Provider may have in any Customer Intellectual Property. Provider shall ensure that all copyright notices and confidentiality legends on all Customer Intellectual Property shall conform to Customer's practices and shall specify Customer as the owner of the work. It is specifically agreed that Customer shall have the full and free right to do or not to do whatever it desires with respect to the Customer Intellectual Property, including without limitation, the right to utilize or not utilize the same, the right to file or not file a patent application and the right to license or sell the same, upon such terms as it may desire, with or without compensation.

4. Payment Obligations.

A. Payment and Invoice. Payment and invoicing terms and obligations shall be as set forth in an Order. Customer agrees that amounts due on all invoices shall be due and payable within thirty (30) days of Customer's receipt of such invoice. Provider reserves the right to charge a late fee of $35 plus a finance charge of one and one half percent (1-1/2%) per month, or the maximum rate permitted by state law, whichever is less, from the date due, on any undisputed required payment that is not made within thirty (30) days of its due date.

B. Expenses. Provider shall be solely responsible for payment of all expenses arising from its provision of the SaaS, including without limitation, expenses for facilities, computer equipment, software, work space, utilities, internet and/or telecommunications charges and management. Customer shall reimburse Provider for all actual expenses incurred by Provider in connection with this Agreement, provided such expenses are pre-approved in writing by Customer. All fees for SaaS will not increase by more than the lesser of the Consumer Price Index ("CPI") of three percent (3%) annually.

5. Confidential Information.

A. Confidential Information**.** Customer acknowledges that the Software and all technical documentation relating thereto provided to Customer in connection with this Agreement and the pricing set forth in this Agreement is the confidential and proprietary information of Provider ("**Provider's Confidential Information**"). Provider acknowledges that all information (whether or not specifically labeled or identified as confidential), in any form or medium (whether in

oral, written, electronic, graphic or other form), that is disclosed to, or developed or learned by, or that becomes known to, Provider or any of its employees (i) in connection with the SaaS hereunder and/or (ii) that relates to the business, operations, products, services, know how, strategies, promotions, research, prospects, employee-relations or development of Customer or its affiliates, franchisees, suppliers, clients or customers is the confidential and proprietary information of Customer ("**Customer Confidential Information**", together with Provider's Confidential Information collectively referred to as "**Confidential Information).** Confidential Information shall not include any information that Recipient can demonstrate by clear and convincing evidence (i) is publicly known through no wrongful act or breach of obligation of confidentiality; (ii) was lawfully known to Recipient prior to the time it was disclosed to, or learned by, Recipient during the term of this Agreement; (iii) was received by Recipient from a third party not in breach of any obligation of confidentiality; or (iv) was independently developed by Recipient without any use of any Confidential Information.

B. Agreement to Maintain Confidentiality. Recipient acknowledges and agrees that Recipient and its employees shall have access and contribute to information and materials of a highly sensitive nature (including Confidential Information) and it shall protect the legitimate business interests of the Discloser therein. Recipient agrees that during the term of this Agreement and at all times thereafter, without the prior written consent of the Discloser, the Recipient shall not use, and shall not permit its employees or consultants/sub-contractors to use, for its or their benefit or the benefit of any other person or entity, and shall not disclose, or permit its employees to disclose, to any other person or entity, any Confidential Information, except to the extent such use or disclosure is required in connection with the performance of services on a Project or pursuant to Section 5(D). Recipient shall use its best efforts and utmost diligence to safeguard the Confidential Information and to protect it against disclosure, misuse, espionage, loss and theft.

C. Material, Non-Public Information. Provider is aware, and Provider will also advise its employees, that applicable securities laws restrict persons with material, non-public information concerning Customer (including, without limitation, Confidential Information) from purchasing or selling securities of Customer or from communicating such information to any other person or entity under circumstances in which it is reasonably foreseeable that such other person or entity is likely to purchase or sell such securities.

D. Required Disclosures. In the event that the Recipient or any of its employees is required by law or court order to disclose any Confidential Information, the Recipient shall (i) promptly notify the Discloser in writing and in no event later than five (5) business days prior to any such disclosure; (ii) cooperate with the Discloser to preserve the confidentiality of such Confidential Information consistent with applicable law; and (iii) use the Recipient's best efforts to limit any such disclosure to the minimum disclosure necessary to comply with such law or court order.

E. Irreparable Harm. The parties agree that any threatened or existing breach of Section 5 of this Agreement would cause the Recipient irreparable injury for which it would have no adequate remedy at law. In each such case, the parties agree that the Discloser shall be entitled to immediate injunctive relief prohibiting such violation, in addition to any other rights and remedies available to the Discloser.

F. Records Retention. Provider shall enable Customer to store and retain I-9s and supporting documents in the Software for all active Customer employees and terminated employees in accordance with I-9 regulatory requirements. As of this signing of this Agreement, U.S. employers are required to maintain I-9s for all current employees. Once an employee is terminated, an employer must maintain the I-9 for a period of three (3) years after the employee was hired or one (1) year after the employee is terminated, whichever is later. As set forth in Exhibit A, Customer may use the Software to view a list of purge-able I-9s which is automatically calculated based on the hire and termination dates entered into the Software by Customer. Upon request, Provider will certify to Customer (and any relevant governmental agency, as applicable) in a mutually agreeable form that the Software enables retention of I-9s in accordance with this section.

6. Testing Period. Intentionally Deleted.

7. Term and Termination.

A. Term. Please see the Order for the initial term ("**Initial Term**"). Any term extension after the Initial Term shall be defined as a "**Renewal Term**"). Unless otherwise specified in an Order, each Renewal Term period shall not be for a length of more than 12 months.

B. Earlier Termination of Agreement.

1. If either party materially breaches any term or condition of this Agreement and fails to cure such breach within thirty (30) days after receiving written notice of the breach, the non-breaching party may terminate this Agreement on written notice at any time following the end of such 30-day period.

2. This Agreement may be terminated by (i) either party, upon the failure of the other party to perform any obligation required to be performed by it hereunder which is not remedied within thirty (30) days of the receipt of written notice thereof; and/or (ii) by Customer, upon a determination by the Department of Homeland Security, Homeland Security Investigations or Immigration and Customs Enforcement, including any successor entities, that Provider's Software is not in compliance with federal immigration laws. Either party may immediately terminate this Agreement in the event that the other party shall (i) cease conducting business in the normal course, (ii) become insolvent, (iii) make a general assignment for the benefit of creditors, (iv) suffer or permit the appointment of a receiver for its business or assets or (v) avail itself of, or become subject to, any proceeding under any bankruptcy, reorganization, arrangement of debt, insolvency, readjustment of debt or receivership law or statute.

3. Intentionally Deleted.

4. Prior to any termination of this Agreement and subject to Customer's payment of all applicable fees and charges, Provider will provide prompt assistance to Customer or another third party in order to provide an orderly transition. In connection with this transition assistance, Provider will: (a) transfer all Customer records and files stored in the SaaS to Customer in an industry standard XML format; (b) cooperate with Customer in the transition from Provider to any third party vendor; and (c) maintain the same service levels during the transition period. If this transition has not been completed by the estimated termination date, Provider will, at the request of Customer, continue to provide the SaaS on a month-to-month basis for up to twelve (12) months from the estimated date of termination, and will continue to be compensated at the same rates then in effect.

C. Return of Materials. Upon the termination of this Agreement, Provider shall return to Customer all Confidential Information (including each and every form and copy of such Confidential Information) and deliver to Customer all Intellectual Property and all other properties of Customer.

8. Provider Warranties.

A. Provider represents and warrants to Customer that (i) it is the lawful owner or licensee of the Software and Provider Materials, and has full legal power and authority to enter into and perform its obligations under this Agreement, (ii) the SaaS provided throughout the term of this Agreement shall conform to the provisions set forth in Exhibit A, with the exception of non-material items, (iii) the Software will operate in substantial conformance with the user documentation supplied by Provider when used in compliance therewith, (iv) the SaaS will be provided using generally accepted industry standards, (v) the SaaS and any component thereof does not violate any applicable law, rule or regulation or any third party, including any patent, trademark, trade name, copyright, trade secret or other intellectual property right. The term "**Provider Materials**" means the Provider environment, including without limitation, the software (in object- or source-code form) and related documentation specified in Exhibit A, the server hardware, disk storage, firewall protection, server operating systems, management programs, and related documentation provided by Provider under this Agreement.

B. Provider represents and warrants that it has the right and authority to enter into, and to grant the rights and perform the obligations described in this Agreement.

C. Provider represents and warrants that the SaaS will be provided in a professional and workmanlike manner, consistent with the skills of an experienced provider of such services and that all deliverables will comply in all material

respects with their specifications for a period of one (1) year from the date of delivery and they will be free from material errors in operation and performance.

D. Provider represents and warrants that it will provide support services as set forth in Exhibit B attached hereto and incorporated herein (the "**Support Services**").

E. Provider represents and warrants that the SaaS will meet or exceed the levels of performance as set forth in Exhibit C attached hereto and incorporated herein (the "**Service Levels**").

F. Provider represents and warrants that the SaaS shall, where applicable, conform to the Department of Homeland Security recordkeeping standards for the generation and storage of electronic Forms I-9 at 8 CFR 274a.2(e) and all related sections as amended by 75 FR 42575-42579, or any successor thereto ("Electronic I-9 Regulations"), which include, but are not limited to,: (i) reasonable controls to ensure the integrity, accuracy and reliability of the electronic generation or storage system; (ii) reasonable controls designed to prevent and detect the unauthorized or accidental creation of, addition to, alteration of, deletion of, or deterioration of an electronically completed or stored Form I-9, including the electronic signature if used; (iii) an inspection and quality assurance program evidenced by regular evaluations of the electronic generation or storage system, including periodic checks of the electronically stored Form I-9, including the electronic signature if used; (iv) a retrieval system that includes an indexing system that permits searches, identification and retrieval for viewing or reproducing of relevant documents and records maintained in the SaaS; (v) the ability to reproduce legible and readable hardcopies of the Form I-9 records; (vi) the ability to retrieve and reproduce (including printing copies on paper, if requested) the Forms I-9 electronically retained in the electronic storage system and supporting documentation along with associated audit trails; (vii) the ability to provide a requesting agency of the United States with the resources (e.g., appropriate hardware and software, personnel and documentation) necessary to locate, retrieve, read, and reproduce (including paper copies) any electronically stored Forms I-9, any supporting documents, and their associated audit trails, reports, and other data used to maintain the authenticity, integrity, and reliability of the records; (viii) the ability to provide, if requested, any reasonably available or obtainable electronic summary file(s), such as a spreadsheet, containing all of the information fields on all of the electronically stored Forms I-9 requested by a requesting agency of the United States; (ix) reasonable controls to ensure that (a) only authorized personnel have access to electronic records; (b) backup and recovery of records is available to protect against information loss, such as power interruptions; (c) Customer employees are trained to minimize the risk of unauthorized or accidental alteration or erasure of electronic records; and (d) information demonstrating whenever the electronic record is created, completed, updated, modified, altered, or corrected, a secure and permanent record is created that establishes the date of access, the identity of the individual who accessed the electronic record, and the particular action taken; and (x) Processes to ensure that all electronic signatures conform to the requirements of 8 CFR 274a.2(h) which require the system to (a) affix the electronic signature at the time of the transaction; (b) create and preserve a record verifying the identity of the person producing the signature; and (c) upon request of the employee, provide a printed confirmation of the transaction to the person providing the signature.

9. Indemnification and Limitation on Damages

A. Indemnification of Customer. Provider shall indemnify, defend and hold Customer, Customer's Affiliates and each of their respective directors, officers, employees, independent contractors and agents (each an "**Indemnified Party**") harmless, if and to the fullest extent permitted by law, from and against:

1. Any actions, lawsuits or proceedings (each, a "**Claim**" and, collectively, "**Claims**"), damages, losses, reasonable attorneys' fees, costs, expenses, liabilities and settlement amounts (each, a "**Loss**" and, collectively, "**Losses**"), against Customer based upon an allegation that the SaaS either infringes, violates, or misappropriates a patent, copyright, trademark, trade secret or other proprietary right of a reasonably anticipated third party; provided, however, that Provider shall not have any obligations under this Section 9A(1) with respect to Losses or Claims incurred or asserted to the extent caused by: (i) Customer's negligence or willful misconduct; (ii) Customer's substantial and/or material modifications to the SaaS not approved by Provider; (iii) Customer knowing and intentional non-compliance with applicable documentation related to the SaaS provided to Customer by Provider; (iv) Customer's use of the SaaS for separate and distinct purposes not contemplated by this Agreement or applicable documentation (including distribution to third parties); (v) Customer's knowing and intentional use or combination of the Provider's software with products, software, or

services that are not provided or approved by Provider; or (vi) Customer's use of the SaaS after Provider notifies Customer to discontinue use because of an infringement claim. "**Customer's Affiliates"** means an entity: (a) controlling; (b) under the control of; or (c) or under common control with Customer.

2. Any Form I-9 fines or penalties imposed by the U.S. Immigration and Customs Enforcement (or successor agency) and paid, even if pursuant to a settlement agreement, by Customer as a direct and sole result of Provider's failure to comply with the Electronic I-9 Regulations. Provider's obligations under this section shall be limited to no more one million dollars (USD $1,000,000).

The Indemnified Party shall be entitled to retain counsel and control the defense of any third party claim ("**Third Party Claim**") subject to indemnification under this Section 9A. In its defense of any such Third Party Claim, the Indemnified Party shall act reasonably and in accordance with its good faith business judgment, which shall include at a minimum, providing Provider with reasonably prompt written notice of any Claim or Loss. Additionally, the Indemnified Party shall not settle or compromise any Third Party Claim without Provider's consent, which consent shall not unreasonably be withheld. All settlement amounts, costs and expenses shall be borne by Provider.

In addition to the indemnity provided above in Section 9(A)(1), if Customer's use of the Software, Provider Provided Equipment (as defined in Exhibit A) or Systems is enjoined, or in the event that Provider desires to minimize its liabilities hereunder, Provider shall:

1. At its cost, obtain for Customer the right to continue their use of the Software, Provider Provided Equipment or Systems on terms no more restrictive than those contained in this Agreement.

2. If the action described in 1 is not possible, even after the use of Provider's best efforts, then Provider, at its cost, shall modify the Software, Provider Provided Equipment or Systems so that it no longer infringes but still is equally suitable and functionally equivalent.

3. If the actions described in 1 and 2 are not possible, even after the use of Provider's best efforts, then Provider shall, at its cost, substitute other equally suitable and functionally equivalent software, equipment or systems.

4. If none of the actions in 1,2 and 3 are available even after Provider's best efforts, Provider may terminate this Agreement upon thirty (30) days written notice to Customer and shall refund to Customer any unused (on a pro-rata basis) fees paid by Customer.

B. Indemnification of Provider. Customer shall, at its own expense and subject to the conditions set forth in this Section 9 with respect to Provider, indemnify and hold Provider, and each of its respective directors, officers, employees, independent contractors and agents harmless from and against any and all claims, demands, actions, suits, prosecutions and other proceedings brought by or on behalf of a third party, and all resulting damages, liabilities, losses, fines, penalties, judgments, awards, settlements, costs and expenses (including reasonable attorneys' fees and costs), directly arising out of or based upon the negligence, intentional misconduct, violation of applicable law, or material breach of this Agreement by Customer or its personnel.

C. Limitation of Damages.

1. Limitation on Types of Recoverable Damages. Neither party shall be liable to the other party hereunder for special, indirect, consequential, exemplary or incidental damages including but not limited to loss of profits, goodwill, use, data loss or other intangible items such as business interruption or the cost of recovering such data even if the party has been advised of the possibility of such damages or losses.

2. Cap on Direct Damages. Except as provided in section 9(C)(3) below and except for damages arising out of a party's indemnification obligations or any other liability which may not be excluded by law, each party's aggregate liability to the other party arising under or in relation to this Agreement, (other than Customer's obligation to pay fees) will be limited to two (2) times the amount Customer paid to Provider in the twelve (12) months preceding the date the Claim giving rise to such liability arises.

3. Exclusions. The limitations described in section 9(C)(2) do not apply to damages arising from or related to (a) either party's breach of section 5 (Confidential Information), and (b) Provider's breach of section 10 (Personal Information, Data Protection, Network Security and Security Assessment) which results in the unauthorized disclosure, access or use of Customer data (each, an "Enhanced Liability"), provided that in any event, the total aggregate liability of a party for an Enhanced Liability shall not exceed USD $25,000.

10. Personal Information, Data Protection, Network Security and Security Assessment.

A. Personal Information.

(1) Under this Agreement Provider will collect, compile, reproduce, store and/or distribute personal information and data (as may be obtained, compiled or developed by Provider, "**Personal Information**"). Unless otherwise agreed to in writing by the Parties, Provider represents and warrants that in collecting, compiling, reproducing, storing and distributing Personal Information: (i) it will store and retain all Personal Information within, and not transmit or permit the transmission of any Personal Information outside of, the United States; (ii) it will only use Personal Information for the sole purpose of performing, and as reasonably necessary to perform, services contemplated by this Agreement; (iii) it will at all times abide by and comply with all of the provisions of its privacy policy for its consumers, as may be in effect from time to time; (iv) except as otherwise permitted by this Agreement and as reasonably necessary to provide services in connection with this Agreement, it shall not use any Personal Information for itself or any third party or otherwise disseminate any Personal Information to any third party without the prior written consent of Customer and the subject individuals; (v) it will use its best efforts and utmost diligence to safeguard the Personal Information and to protect it against disclosure, misuse, espionage, loss and theft; and (vii) it shall at all times comply with all applicable laws and regulations governing privacy, data gathering and unsolicited commercial e-mail.

(2) Provider represents and warrants that it will, to the extent Provider receives, stores, maintains, processes, or otherwise is permitted access to, Personal Information of residents of the Commonwealth of Massachusetts, implement and maintain appropriate security measures to protect such Personal Information which are consistent with and meet the requirements of 201 CMR 17.00.

B. Data Protection.

(1) Provider shall establish and maintain physical, technical, and administrative safeguards that are reasonably designed and implemented to protect against and detect the unauthorized access, disclosure, transmission, destruction, loss, alteration or theft of any Confidential Information and Personal Information utilized by Provider (or its Sub-Contractors) in connection with its performance of the SaaS. Such measures shall (i) include, at a minimum, using firewalls, intrusion detection, password protection and Malware protection software, and performing periodic, but in any event at least annual, internal security audits of Provider's and its Sub-Contractors' (if applicable) systems and the SaaS and tests of applicable disaster recovery and business continuity plans and facilities and (ii) be compliant, at a minimum, with industry standards. Such security measures shall ensure the security and confidentiality of Confidential Information and Personal Information, protect against any anticipated threats or hazards to the security or integrity of Confidential Information and Personal Information, comply with applicable laws, including those relating to data security and the handling of data security breaches, and otherwise protect against unauthorized access to or use of Confidential Information and Personal Information. "**Malware**" means any virus, Trojan horse, worm, spyware (such as, any program that tracks the computer's use in some manner, including downloaded files or usernames and passwords for websites or programs), adware (such as, any program that connects to the Internet and uses the computer to host advertisements and/or possibly transmit advertisements to other computers) or other code designed or used to disable, erase, alter, or otherwise harm any computer system, program, database, data, hardware or communications system, or to consume, use, allocate or disrupt any computer resources, in a manner which is malicious or intended to damage or inconvenience. In the event Provider determines through a security review process that Provider's security measures reveal a security risk which can reasonably be classified as "high" or "medium" according to industry standards, Provider agrees to remediate such deviations within a reasonable period of time.

(2) No media on which Confidential Information or Personal Information is stored may be used or re-used to store data of any other customer of Provider or to deliver data to a third party, including another of Provider's customer, unless securely erased.

(3) Provider will promptly retrieve and deliver to Customer a copy of all Confidential Information and Personal Information (or such portions as will be specified by Customer) in an industry standard XML format: (i) at Customer's reasonable request from time to time; (ii) upon termination or expiration of the Term or a Project; or (iii) with respect to particular Confidential Information or Personal Information, at such earlier date that such information is no longer required by Provider to perform the Services. Thereafter, if requested by Customer, Provider will destroy or securely erase all copies of Confidential Information and Personal Information in Provider's (or its Sub-Contractors') possession or under Provider's (or its Sub-Contractors') control. Provider will not withhold any Confidential Information or Personal Information as a means of resolving any dispute.

(4) If Provider is requested or required by law to disclose any Personal Information, Provider shall not disclose the Personal Information without complying with the provisions of applicable laws and providing Customer notice of such request within forty-eight (48) hours of receiving it so that Customer may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure, including, but not limited to, seeking a protective order. Notwithstanding the foregoing, Provider shall exercise all reasonable efforts to prevent or limit any such disclosure or to otherwise preserve the confidentiality of Personal Information including, without limitation, by cooperating with Customer to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Personal Information.

(5) Provider agrees that if Customer should provide written consent to Provider permitting it to disclose Personal Information to any third party, Provider will have in place written agreements with any such third party to whom Provider or any Worker discloses Personal Information ensuring that such third party is bound by the same obligations as Provider under this Agreement. Provider shall remain accountable and responsible for any actions by such third parties.

C. Intentionally Deleted.

D. Intentionally Deleted.

E. Subcontractors.

Provider may engage subcontractors to assist in its performance hereunder, including but not limited to the performance of web hosting services. Provider shall at all times be the primary party responsible for its performance hereunder, and shall have ultimate responsibility and liability for its subcontractors' performance.

11. Miscellaneous.

A. Applicable Law. This Agreement shall be governed by the internal laws of the State of Illinois, without giving effect to conflict of law principles, except that the current proposed Uniform Computer Information Transaction Act (formerly proposed Article 2B to the Uniform Commercial Code) nor any version thereof ("**UCITA**") shall not apply to this Agreement or any Ordering Document.

B. Additional Expenses**.** Customer shall not incur any additional fees or expenses beyond those set forth in this Agreement unless expressly agreed to in writing by Customer.

C. Intentionally Deleted.

D. Remedies Cumulative. Except for those sections in this Agreement that contain exclusive remedies, all remedies of Customer provided for in this Agreement shall be cumulative and in addition to and not in lieu of any other remedies available to Customer at law, in equity or otherwise.

E. Severability**.** Any invalidity, in whole or in part, of any provision of this Agreement shall not affect the validity of any other of its provisions.

F. Notices**.** Any notice or other communication hereunder shall be in writing by certified or registered mail or by personal delivery. Any such notice shall become effective only upon receipt at the addresses stated in the Order, which upon written notice, may be changed from time to time.

G. Entire Agreement**.** This Agreement, together with all other exhibits attached hereto or referenced herein, constitutes the entire agreement between the parties hereto and supersedes and preempts any prior understandings, agreements, representations or statements of any kind, oral or written, that may have related to the subject matter hereof in any way. The parties also understand, acknowledge and agree that unless otherwise specified in a written instrument signed by an officer of both parties no additional terms or changes to these terms, even if such additional terms or changes contain provisions to the contrary, shall be valid or binding on the parties. Additionally, the parties specifically agree that any language or provisions contained in any "shrinkwrap" or "clickwrap" agreement shall be of no force and effect if such provisions conflict with the terms of this agreement.

H. Waiver**.** No term or provision hereof shall be deemed waived and no breach excused unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented.

I. Assignment**.** This Agreement shall be binding on the parties hereto and their respective successors and assigns. Neither party may, or shall have the power to, assign this Agreement without the prior written consent of the other, such consent not to be unreasonably withheld.

J. Use of Marks and Names. Each party agrees that it will not use the name, trademark, service mark, or trade name of the other party, its divisions, subsidiaries, or affiliates in publicity releases, promotional material, promotional media or written advertising, including customer lists, without the prior written consent of an officer of the other party.

K. Force Majeure Events. Neither party shall be liable for any delays in its performance hereunder resulting from circumstances or causes beyond its reasonable control, including, without limitation, fire or other casualty, act of God, Internet or power outages, telecommunications outages, acts or threatened acts of terrorism, pestilence or epidemic, strike or labor dispute of a third party, war or other violence, or any law, order or requirement of any governmental agency or authority, provided the delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented through the use of a reasonable security and disaster recovery plan, and provided further that the party hindered or delayed immediately notifies the other party describing the circumstances causing the delay.

EXHIBIT A

Description of SaaS

The Guardian solution by LawLogix ("Guardian") enables organizations to complete and retain an entirely electronic version of the Form I-9, a government form which must be completed by all employers to document their new hires' eligibility to work in the United States. As part of the I-9 process, employees will complete and sign section 1 of the form (containing mostly biographic information) and present original identity and work authorization documents to the employer to prove that they are authorized to work in the U.S. The employer then must record the document information in section 2 and sign the form. Some of the primary advantages of using the Guardian electronic I-9 system is that it prevents errors or omissions on the form, tracks important deadlines, seamlessly transmits information to E-Verify as applicable, centrally stores and manages both electronic and historical paper forms, and generates reports needed to ensure compliance.

Software Features

Electronic I-9 Completion

- Web-based electronic interface enables employees and employer representative to electronically complete and store the Form I-9
- Real-time error checking prevents I-9 compliance mistakes or omissions based on the I-9 regulations and current government handbooks (e.g., the "M-274 Handbook for Employers")
- Prevents duplicate or inaccurate social security numbers (based on SSA's numbering rules)
- Customizable help-text enables organization to write specific instructions for each field on the Form I-9
- Bilingual English/Spanish view of section 1 of the I-9
- Newly created electronic I-9s will always use the latest version available on the USCIS website
- I-9s cannot be marked "completed" until all errors have been resolved
- Special I-9 rules guide employees who are under the age of 18 ("minors") and are unable to present an identity document
- Ensures the use of the latest (correct) version of the Form I-9
- Prevents the most common example of over-documentation in section 2 (recording documents in List A, B, and C) while ensuring the document presented corresponds with the employee's attestation in section 1
- Ability to scan copies of documents used in verification and attach them to the individual employee's record

Reverifications

- Reverify expiring work authorization documents for certain foreign national employees by completing section 3 or a new I-9
- A Section 3 entry is always completed on the latest version of the Form I-9
- Ability to perform multiple reverifications on each employee when permissible

Electronic Signature

- Section 1 features a proprietary identity-verification based electronic signature methodology which is designed to unequivocally capture the employee's intent to sign
- Sections 2 and 3 of the I-9 can be signed by the employer representative using a secure password
- All electronic signatures are captured in the audit trail

E-Verify and FAR Functionality

- Enable E-Verify by location or FEIN
- Data from completed and approved I-9s is electronically submitted to E-Verify and responses are instantly viewable in the Software
- Ability to process an E-Verify mismatch as required under the E-Verify Memorandum of Understanding (MOU), including electronic signature and retention of the TNC notices and letters
- Integrated photo matching tool enables comparison of E-Verify photo with the employee's ID uploaded to the Software
- Proprietary E-Verify FAR functionality enables covered federal contractor to manage federal contracts in the Software, attach contracts to affected employees, check historical I-9s for E-Verify compatibility, and batch submit through the Guardian FAR queue.

Dashboard

- Dashboard provides comprehensive view of important I-9 and E-Verify deadlines, based on the user's permissions
- Available dashboards include pending I-9s, pending reverifications, I-9s needing further action, pending E-Verify actions, I-9s needing approval, and employee counts (among others).
- Pending I-9s feature color-coded compliance visuals based on I-9 compliance deadlines
- Ability to directly access employee, I-9, and E-Verify records (as applicable)

Ability to correct I-9s

- Ability to makes corrections and exemptions to I-9s according to current DHS/ICE standards.
- Option to require all section 1 changes to be made by the employee
- Amended I-9s display corrected data in a different color font, along with user user's initials and date of correction

Remote Hiring

- Secure login enables new hires to complete Section 1 of the I-9 remotely
- Remote third-party can complete Section 2 of the I-9 through a one-time system access
- Employer can easily review and approve remotely completed I-9s to ensure accuracy

Reports

- Comprehensive list of "canned" reports can be generated by employer representatives
- Reports display records based on user's permission
- Interactive report features drag/drop functionality, enabling employer to query/view any field on the I-9, employee, or E-Verify record.
- Reports can be saved, re-used, and made public/private
- Ability to graphically report and track the timeliness of all I-9 and E-Verify transactions

Audit Trail

- The Software creates a secure and permanent record of every I-9 and E-Verify event which occurs in the system. Specifically, Guardian records every time an I-9 is created, completed, updated, modified, altered or corrected with the following corresponding details:
- Ability to graphically report and track the timeliness of all I-9 and E-Verify transactions
- Name of employee/record for which the data was change
- Type of event (i.e. addition, update, etc.)
- Date and time stamp (down to the second)
- Name of the user who made the change
- The button clicked (or action taken to make this record an event)
- The field that was altered
- The old data (if there was any)
- The new data (if any was added)

I-9 Retention

- Detailed and reportable history of I-9 creation
- Calculation of the "purge date" based on 3- and 1-year rule and ability for administrators to purge multiple I-9s
- When deleting purge-eligible records, each I-9's entire associated history is purged with it.

Product and Industry Updates

- Upcoming I-9 and E-Verify regulatory changes are communicated via a Provider blog and email notification to the users
- Links to software-embedded tutorials are included with uploaded system changes

Overview of Services

Provider may offer Customer additional and related services, which include but are not limited to: Data Migration of Customer's Pre-Existing I-9 Records ("**Data Migration**" or "**Additional Services**").

Description of Data Migration

Provider shall convert and migrate electronic client data or paper data on Customer's behalf, which includes the upload of I-9 data and associated audit trails (if any) as well as scanned copies of signed paper I-9s into the Software, as applicable pursuant to a separate Statement of Work. Prior to data migration, Customer and Provider shall consult and agree upon any data restrictions, limitations and/or exclusions. Within the limitations of the data structure present in the supplied data file and as possible within the constraints of the exporting software program or the paper based files, as applicable, Provider will engineer migration routines or implement manual data entry efforts so as to migrate the usable data from Customer's current system into the Software and make the data along with scanned I-9s and any supporting documentation available to Customer within a mutually agreed upon time frame. Upon completion of the migration, Provider will generate, on behalf of Customer, a report which includes a technical estimated compliance summary (TECS) of the migrated I-9s. This summary is a tabulation and categorization (data analysis) that highlights those I-9s that appear to be incomplete, incorrect, or otherwise not in compliance. The summary is "data-centric" which means that while the final report (and access to the actual I-9 data within Guardian) is very valuable, the report is only a jumping-off point for legal review or corrections and not a definitive legal or analytical determination. Upon completion of the migration, Customer may utilize a Batch E-Verify processing submission for those migrated I-9s for which E-Verify is applicable and allowable.

Overview of Integrations

As part of an I-9 subscription plan, Provider may facilitate the sharing of certain employee and/or I-9 information between Guardian and Customer's human resource application(s) (hereinafter an "Integration") as more specifically set forth in an Order. By way of example, and not limitation, an Integration may permit the automated creation of an employee record in Guardian for all new hire employees who require an I-9 (based on onboarding information sent from Customer's onboarding platform).

EXHIBIT B

Support Services

USER TYPES AND CUSTOMER SUPPORT.

Provider shall provide customer support in conformance with the customer support policies defined in this section. Provider reserves the right to make changes to the policies, procedures and practices regarding support services upon written notice, provided such changes do not materially affect the overall level, including both quality and/or quantity of the support services provided to Customer.

(a) User Types. Access for Authorized Users can be added in the SaaS as Basic Users, Standard Users, or Premium Users as defined herein.

(i) "Basic Users" can perform, as applicable, the creation, editing, and viewing of Customer's I-9 records through a simplified Software interface which is designed for store managers. Customer can add or create an unlimited number of Basis Users.

(ii) "Standard Users" can perform, as applicable, the creation, editing, viewing, and reporting of Customer's I-9 records through a full-featured user interface as well as submitting I-9s to E-Verify. Customer can add or create an unlimited number of Standard Users.

(iii) "Premium Users" can perform all of the activities of a Standard User; select Software preferences; add users and user groups; train Customer's Users on E-Verify; add locations and corporate entities; establish user assignments; and otherwise administer the Software for Customer.

(b) Customer Support. During the Term of this Agreement, Provider shall:

(i) Provide on-line customer service support ("Support") to the specified number of Premium Users in an Order at no charge during the designated customer service hours of 6:30am to 6:00pm (Mountain Standard Time), Monday through Friday excluding the following Provider recognized holidays: New Year's Day, Memorial Day, Independence Day (4th of July), Labor Day, Thanksgiving, the day after Thanksgiving, and Christmas Day. In the event a holiday falls on a weekend, Provider will treat the preceding or subsequent weekday as a holiday instead (exact schedule will be made available to Customer in advance).

(ii) Intentionally Deleted.

(iii) Intentionally Deleted.

(iv) Log every service call received from Customer, along with actions taken by Provider to provide a solution, if applicable and available.

(v) Use commercially reasonable efforts to respond to Software support requests from Premium Users based on the severity level of the issue (as determined in good faith by Provider) in accordance with the Service Level Agreement attached hereto as Exhibit B. Provider does not guarantee resolution times, and a resolution may consist of a fix, workaround, service availability, or other solution to restore functionality. Customer acknowledges and agrees that the response protocol described herein does not apply to general usage questions, documentation errors, issues related to a non-production environment, or feature requests reported by Customer.

EXHIBIT C

Service Levels

Provider represents and warrants that it shall provide the SaaS twenty-four (24) hours a day, seven (7) days a week throughout the Term of this Agreement. Customer agrees that from time to time the SaaS be inaccessible or inoperable for various reasons limited to (i) periodic maintenance procedures or repairs which Provider may undertake from time to time; (ii) causes which are beyond the control of Provider or are not reasonably foreseeable by Provider, including interruption or failure of telecommunication or digital transmission links, network congestion, or hostile network attacks ((iii) the pre-approved nightly maintenance window during the hours of 10:00pm to 4:00am Arizona time, when the SaaS might be unavailable for maintenance or the deployment of system enhancements ("Regularly Scheduled Maintenance")(collectively "Downtime"). During each period of Regularly Scheduled Maintenance, any user attempting to access the Software will be notified via an automated status screen in the Software that the Software is unavailable due to maintenance. Provider shall use its best efforts to minimize any disruption, inaccessibility and/or inoperability of the SaaS in connection with Downtime, whether scheduled or not.

Provider represents and warrants that the SaaS provided herein will be provided on a twenty-four (24) hours a day, seven (7) days a week basis at an availability of (99%) per month. Downtime will exclude Regularly Scheduled Maintenance, and circumstances beyond the reasonable control of Provider, which shall include (a) problems associated with Customer's hardware, software and Customer's network access or Internet Service Provider; (b) Customer's use of an operating system, web browser, or third party application which is not supported by Provider for the Software as specified in Provider documentation; (c) issues solely associated with third party hosting solutions or services such as the E-Verify system or Customer's onboarding platform; (d) the flow of data to or from Provider's servers and other portions of the Internet which depend on the performance of Internet services provided or controlled by third parties; (e) Force Majeure as defined in the Agreement; and (f) down periods resulting from misuse of the Software by Customer.

The availability of the SaaS for a given month ("SLA Availability") will be calculated according to the following definitions and formula.

$$\frac{\text{Total number of minutes in a month} - \text{Downtime}}{\text{Total number of minutes in a month}} \times 100$$

Should Provider fail to meet the SLA Availability, Provider will credit, upon Customer's request within thirty (30) days of the end of a calendar month measurement period, Customer's account an amount equal to a percentage of the total monthly fee paid by Customer as set forth in the table below. Provider will calculate any service level Downtime using Provider's system logs and other records. The credits set forth in this Section are Customer's exclusive remedy related to Provider's guaranteed uptime.

Percentage of Uptime in Given Month	**SLA Credit**
98.5 to 98.9%	5% of total monthly fee
96.5 to 98.4%	10% of total monthly fee
95 to 96.4%	15% of total monthly fee
< 95%	20% of total monthly fee

Provider may change any of the foregoing contact information from time to time by delivery of not less than thirty (30) days prior written notice to Customer, so long as at least one number or address is at all times available for each means of contact.

***Response Protocol*:**

In the event that Customer reports to Provider an Error in the SaaS (the Severity Level to be reasonably determined by Provider), Provider shall respond to such reports as follows:

Severity Level	Definition	Response
1 – Critical	The Software is inaccessible or so severely impacted that Customer cannot reasonably use the Software. A Severity Level 1 issue could have the following characteristics: • More than 50% of Customer users cannot access the Software • Customer users cannot create or save I-9 records • Customer users cannot submit to E-Verify solely as a result of an error in the Software (i.e., issue is not caused by the E-Verify system itself)	Provider will acknowledge the issue within two (2) business hours of receiving notification from Customer and handle as the highest priority until the issue is resolved.
2 – Significant	Major functionality or performance of the Software is impacted and no reasonable workaround exists. A Severity Level 2 issue could have the following characteristics: • Severely degraded performance • Frequent interruptions in service • Functionality is unavailable but the Software is able to operate in a restricted fashion	Provider will acknowledge the issue within four (4) business hours of receiving notification from Customer and commit full-time resources to resolve. If Provider delivers an acceptable workaround instead of a solution, the severity classification will drop to a 3 – Minimal.
3 – Minimal	A Software feature is unavailable but a workaround exists and the majority of functions are still useable. A Severity Level 3 issue could have the following characteristics: • A particular feature (such as a dashboard) is not working properly, but Customer user can obtain the same information through a report • Minimal Software performance degradation	Provider will acknowledge the issue within two (2) business days of receiving notification from Customer and use reasonable efforts to resolve.

Provider Response to a Government Audit. In the event that Customer reports to Provider the receipt of a Notice of Inspection ("NOI") from the U.S. Immigration and Customs Enforcement (or successor agency), Provider shall make initial contact with Customer within 4 business hours of such report to discuss the NOI and plan for a response and agree on the information needed for Provider to respond. Customer shall provide Provider with a copy of the NOI as well as any additional instructions concerning the affected Customer entities and job locations (based on Customer unique setup). Within 24 hours of receiving all of the agreed upon necessary information and NOI details from Customer, Provider shall provide Customer with a customized export of the relevant I-9 records and supporting documents separated by a cover sheet as well as any additional documentation requested by the inspecting government agency (together, "the Audit

Files"). Provider shall deliver the Audit Files to Customer via secure electronic delivery or optional courier service at Customer expense. Notwithstanding the above, Customer acknowledges and agrees that the employment eligibility verification obligations of Section 274A(b) of the Immigration and Nationality Act rest exclusively with Customer, and nothing in this Agreement is intended to outsource this responsibility to Provider.