Agenda Item #9

INTEROFFICE MEMORANDUM

TO	Mayor Blad & City Council Members
FROM	Abby Newell, Human Resources Generalist
DATE	October 28, 2025
SUBJECT	Executive Summary: Background Check Vendor Change

The Human Resources Department has received direction from City Council following the October 9, 2025 Work Session to transition the City of Pocatello's background check services from Background Investigation Bureau, LLC (BIB) to VerifiedFirst.

VerifiedFirst has agreed to match the City's current pricing while expanding the scope of services to include federal background checks. Additionally, VerifiedFirst offers seamless integration with the City's applicant tracking system, KeldairHR, which will improve efficiency and streamline the hiring process.

Supporting documentation is attached for Council consideration. Council may wish to approve the End User Agreement with VerifiedFirst and authorize the Mayor's signature on all applicable documents, subject to Legal Department review.

911 N 7th Avenue
PO Box 4169
Pocatello, ID 83205

Office: (208) 234-6170
Fax: (208) 234-6572

www.pocatello.gov
HR@pocatello.gov

To: City Council and Mayor

From: Matt Kerbs, Deputy City Attorney MK

Date: October 27, 2025

Re: Verified First End-User Agreement

I have reviewed the above referenced documents and have no legal concerns with the Council approving and authorizing the Mayor to sign the agreement with Verified First, LLC regarding background check services.

Verified First

1. Includes Sex Offender, Global Homeland Security, and Office of Foreign Asset Control database searches. 2. Individual products billed at quoted price. Prices exclude any pass-through, access, or data fees. 3. Address history from credit headers, utilities, etc. Does not determine the eligibility of employees to work in the U.S. Crosschecks with Social Security Death Index. 4. Counties listed on Social Security Address Trace. Prices exclude any pass-through, access, or data fees. 5. Certain industries capped at three counties.

Standard Criminal Package	**Price**
Social Security Address Trace	$2.25
Nationwide Sex Offender Registry	$2.65
Nationwide Criminal Database	$8.00
County Criminal Records	$8.55
Federal Criminal Records	$6.25
Total	**$27.70**

Services to be Enabled	Price
Social Security Address Trace Reveals address history based on credit applications, utility bills, and similar filings. (2)	$2.25
Nationwide Sex Offender Registry Search of the National Sex Offender Registry.	$2.65
Nationwide Criminal Database Multi-jurisdictional search of millions of state and county records. Database is compiled from counties, department of corrections and administrative courts.	$8.00
County Criminal Records - 7 Year Lookback Uncovers misdemeanors and felonies within a specific county's Central or County Seat court. Excludes any pass-through fees. (1)	$8.55
Federal Criminal Records: District of Residence (Only Enabled if Needed) Cases involving: white-collar crimes, embezzlement, kidnapping, illegal sale of firearms, pornographic exploitation of children, drug trafficking. (1)	$6.25
State Criminal Records (Only Enabled if Needed) Checks available counties within the state. Not available in all states. Excludes any pass-through fees. (1)	$17.50

All prices are per name, per search, unless otherwise noted. The pricing being offered is based off of an average monthly volume

of 20 orders placed.

Background Screening Footnotes:

1. Individual products billed at quoted price. Prices exclude any pass-through, access, or data fees.
    1. Individual products billed at fixed-fee price. Excludes any pass-through, access, or data fees.
2. Address history from credit headers, utilities, etc. Does not determine the eligibility of employees to work in the United States. Crosschecks with Social Security Death Index.
3. Counties listed on Social Security Address Trace. Prices exclude any pass-through, access, or data fees.
4. Certain industries capped at three most recent counties. Prices exclude any pass-through, access, or data fees.
5. Fee charged per individual verification. Three attempts made at each reference. Prices exclude any pass-through, access, data fees.
6. Credit Inspection required to meet Federal regulations. One-time $95 inspection fee.
7. The Vaccine Fee will vary from clinic to clinic. This fee will be passed through on the invoice.

VERIFIED FIRST END-USER AGREEMENT

Version 2.2 – November 1, 2024

THIS END-USER AGREEMENT ("Agreement") is made and entered into by and between Verified First, LLC, an Idaho Limited Liability Company with offices at 1120 S Rackham Way, Meridian, Idaho 83642. its subsidiary and affiliate corporations, successors, and assigns ("Company") and: _____ (legal business entity name) doing business as_____ (hereafter "End-User"). This Agreement shall be effective on the date of first signature below (the "Effective Date") provided a countersignature is obtained.

1.General

End-User is engaged in the business of _____ End-User represents and agrees that it is a legal entity in good standing with a legitimate permissible purpose for requesting the Services offered by Company (see Verified First's FCRA Notice to Users).

In connection with the Services (as such term is defined at **www.verifiedfirst.com/definitions**) provided pursuant to the terms of this Agreement, Company strives to deliver accurate and timely "consumer reports" and/or "investigative consumer reports" (collectively "consumer reports") to assist End-User in making intelligent and informed decisions for a permissible purpose under applicable law. To this end, Company assembles information from a variety of sources, including databases maintained by consumer reporting agencies containing information from public records, other information repositories and third-party researchers. End-User understands that these information sources and resources are not maintained by Company. Therefore, Company does not guarantee that the information provided from these sources is accurate or current. Nevertheless, Company has in place reasonable procedures designed to respond promptly to claims of incorrect or inaccurate information in accordance with applicable law.

2.End-User's Certification of Fair Credit Reporting Act (FCRA) Permissible Purpose(s)

a) End-User hereby certifies that each time a consumer report is requested, all of its orders from Company shall be made, and the resulting consumer reports shall be used, for the following Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.,* permissible purposes only (Please select 'Yes' for all that apply):

i) **for employment purposes**, defined as the purpose of evaluating a consumer for employment, promotion, reassignment, or retention as an employee, including contractors and volunteers (§ 1681b-(a)(3)(B)), with the written authorization of the consumer.

ii) **for consumer reports on applicants and tenants** who apply to rent housing or renew a lease, to be used only for housing purposes (qualifies under § 1681b-(a)(3)(F), with the written authorization of applicant or tenant.

iii) Where there is a **legitimate business need**, in connection with a business transaction that is initiated by the consumer (§ 1681b-(a)(3)(F)(i)).

b) End-User will certify the specific permissible purpose each time a consumer report is requested.

3.End-User's Certification of Legal Compliance

a) End-User certifies to Company that the consumer reports it receives will not be used in violation of any applicable federal, state or local laws, including, but not limited to the FCRA and Title VII of the Civil Rights Act of 1964. End-User accepts full responsibility for complying with all such laws, including any state consumer reporting laws or requirements, and for using the consumer reports it receives from Company in a legally acceptable fashion. To that end, End-User agrees to comply with and provide all statutorily required notices under the FCRA or other state laws when using consumer reports. End-User further accepts full responsibility for any and all consequences of use and/or dissemination of those consumer reports. End-User further agrees that each consumer report will only be used for a one-time use.

b) End-User agrees to have reasonable procedures for the fair and equitable use of consumer reports and to secure the confidentiality of private information. End-User agrees to take precautionary measures to protect the security and dissemination of all consumer report or investigative consumer report information including, for example, restricting terminal access, utilizing passwords to restrict access to terminal devices, and securing access to, dissemination and destruction of electronic and hard copy reports. End-User agrees to abide by Addendum A attached hereto which is incorporated into and is part of this Agreement. By using a Company Service, End-User acknowledges and understands the practices described in Company's Privacy Policy and the actual collection, use, and disclosure of End-User-furnished information in accordance with Company's Privacy Policy available at https://legal.verifiedfirst.com/#/legal#privacy-policy.

c) As a condition of entering into this Agreement, End-User certifies that it will comply with all applicable local, state and federal laws including but not limited to the FCRA and state law equivalents. Company will only keep information it provides to End-User for the lesser of two (2) years or as required by applicable law. End-User certifies that it will retain information it receives from Company in accordance with applicable law and will make such information available to Company upon request. In addition, End-User agrees to abide by all state and local "Ban the Box" and other fair chance laws and ordinances, and certifies that it will not conduct a criminal history background check until after conditional offer of employment has been provided, if required by applicable law. If End-User requests and receives a consumer report that contains social media information, End-User certifies that it will not make any decision based on a grade, score, or other notation about the social media information, but will look at the context of all reported information and will follow applicable laws on the use of social media information.

d) If End-User seeks credit information, it certifies to Company that it has obtained written authorization and provided all disclosures required by applicable federal, state or local laws, regulations and ordinances to the consumer in connection with such requests and will provide information and agree to Addendum B before Company can provide credit information to End-User. Addendum B is incorporated into and is part of this Agreement, if applicable. End-User acknowledges and agrees to notify its employees that End-User can access credit information only for the permissible purposes listed in the FCRA.

e) End-User understands that the credit bureaus require specific written approval from Company before the following persons, entities and/or businesses may obtain credit reports: private detectives, private detective agencies, private investigative companies, bail bondsmen, attorneys, law firms, credit counseling firms, security services, members of the media, resellers, financial counseling firms, credit repair clinics, pawn shops (except companies that do only Title pawn), check cashing companies (except companies that do only loans, no check cashing), genealogical or heir research firms, dating services, massage or tattoo services, businesses that operate out of an apartment, individuals seeking information for their own private use, adult entertainment services of any kind, companies that locate missing children, companies that handle third party repossession, companies seeking information in connection with time shares, subscriptions companies, individuals involved in spiritual counseling or persons or entities that are not an End-User or decision maker.

f) End-User represents that, if it orders credit reports, End-User will have a policy and procedures in place to investigate any discrepancy in a consumer's address when notified by the credit bureau that the consumer's address, as submitted by End-User, substantially varies from the address the credit bureau has on file for that consumer.

g) End-User hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, Appendix A) and Notice of Users of Consumer Reports (16 C.F.R. Part 601, Appendix C), and Remedying the Effects of Identity Theft available at **www.verifiedfirst.com/fcra-notifications**.

h) End-User hereby certifies that, under the Investigative Consumer Reporting Agencies Act ("ICRAA"), California Civil Code Sections 1786 et seq., and the Consumer Credit Reporting Agencies Act ("CCRAA"), California Civil Code Sections 1785.1 et seq., if the End-User is located in the State of California, and/or the End-User's request for and/or use of consumer reports pertains to a California resident, applicant or employee, End-User will do the following:

Request and use consumer reports solely for permissible purpose(s) identified under California Civil Code Sections 1785.11 and 1786.12.

i) When, at any time, consumer reports are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, provide a clear and conspicuous disclosure in writing to the consumer, which solely discloses: (1) that a consumer report may be obtained; (2) the permissible purpose of the consumer report; (3) that information on the consumer's character, general reputation, personal characteristics and mode of living may be disclosed; (4) the name, address, telephone number, and website of the Consumer Reporting Agency conducting the investigation; and (5) the nature and scope of the investigation requested, including a summary of the provisions of California Civil Code Section 1786.22.

ii) When, at any time, consumer reports are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, only request a consumer report if the applicable consumer has authorized in writing the procurement of the consumer report.

iii) When consumer reports are sought in connection with the hiring of a dwelling unit, notify the consumer in writing that a consumer report will be made regarding the consumer's character, general reputation, and personal characteristics. The notification shall include the name and address of End-User as well as a summary of the provisions of California Civil Code Section 1786.22, no later than three days after the date on which the consumer report was first requested.

iv) Provide the consumer a means by which the consumer may indicate on a written form, by means of a box to check, that the consumer wishes to receive a copy of any consumer reports that are prepared.

v) If the consumer wishes to receive a copy of the consumer report, the End-User shall send (or contract with another entity to send) a copy of the consumer report to the consumer within three business days of the date that the consumer report is provided to End-User. The copy of the consumer report shall contain the name, address, and telephone number of the person who issued the report and how to contact them.

vi) Under all applicable circumstances, comply with California Civil Code Sections 1785.20 and 1786.40 if the taking of adverse action is a consideration, which shall include, but may not be limited to, advising the consumer against whom an adverse action has been taken that the adverse action was based in whole or in part upon information contained in the consumer report, informing the consumer in writing of Company's name, address, and telephone number, and provide the consumer of a written notice of his/her rights under the ICRA and the CCRAA.

vii) Comply with all other requirements under applicable California law, including, but not limited to any statutes, regulations and rules governing the procurement, use and/or disclosure of any consumer reports, including, but not limited to, the ICRA

and CCRAA.

i) When Consumer Reports are Used for Employment Purposes

i) If the consumer reports End-User obtains from Company are to be used for an employment purpose, End-User certifies that prior to obtaining or causing a "consumer report" to be obtained, a clear and conspicuous disclosure, in a document consisting *solely of the disclosure*, has been made in writing to the consumer explaining that a consumer report may be obtained for employment purposes. Such disclosure satisfies all requirements identified in the FCRA. End-User also certifies that the consumer has authorized, in writing, the obtaining of the report by End-User. If an investigative consumer report (as defined by the FCRA) is obtained, End-User certifies a separate disclosure will be obtained and such disclosure satisfies all requisite disclosure requirements for investigative consumer reports. End-User certifies that it also has provided the consumer with any notices or disclosures required under applicable state and local law. End-User understands and agrees that Company will not initiate a report for employment purposes in the absence of a written authorization. End-User certifies that each time it orders a report, it is reaffirming the above certifications.

ii) Prior to taking adverse employment action based in whole or in part on the consumer reports provided by Company, End-User will provide to the consumer: (1) a copy of the report, and (2) a description, in writing, of the rights of the consumer entitled: "A Summary of Your Rights Under the Fair Credit Reporting Act." After the appropriate waiting period, End-User will issue to the consumer notice of the adverse action taken, including the statutorily required notices identified in Section 615 of the Fair Credit Reporting Act. End-User will not initiate the pre-adverse and adverse action notice process until Company has completed all search components of the consumer and/or investigative consumer report, Company has provided the complete report to End-User, and End-User has reviewed the consumer report contents. End-User also will not initiate the pre-adverse and adverse action notice process or otherwise take adverse action against a consumer based on a search or component of a search that is canceled, not completed, unable to be performed, or marked as unperformable or that receives any other mark or notation indicating that the search is not "complete."

iii) Before taking adverse action based on a criminal record the EEOC Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions recommends that you perform an individualized assessment and or other considerations. To obtain a copy of this EEOC Enforcement Guidance please go to the following website: **http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm**.

iv) Please note, as it relates to criminal history information, Company only reports conviction records and will report a minimum of seven (7) years of conviction information, where allowed by any applicable fair credit reporting laws. Company does not report non-conviction information unless a case is pending with a next court date scheduled and does not report information relating to infractions, summary offenses, violations or other sub-criminal information. In determining whether a criminal record is reportable, Company does not apply any state or local laws restricting the employer use of criminal history UNLESS END-USER PROVIDES ADDITIONAL REPORTING RESTRICTIONS TO BE APPLIED TO CONSUMER REPORTS. End-User assumes full responsibility for determining whether reported information may be used in the jurisdiction where the consumer lives, works, or is applying for work.

v) Company complies with all FCRA and state and local laws that restrict the reportability of certain types of adverse information about a consumer. To ensure compliance with such laws, End-User acknowledges and agrees that when including any information about a consumer in a consumer report, Company follows the most restrictive reporting restrictions based on the consumer's residence address. End-User understands that some state laws allow Company to report convictions where the date of disposition is older than seven years provided the consumer residing in the state is being considered for a position with an annual salary that equals to, or is reasonably expected to equal, $25,000 or more. End-User certifies that if it seeks to have access to convictions with a disposition date that is older than seven years, such information will only be sought for consumers applying for employment with End-User who are being considered for a position with an annual salary that equals, or is reasonably expected to equal, $25,000 or more.

j) When Consumer Reports are Used for the Permissible Purpose of Tenant Screening

End-User certifies that it will obtain written authorization from the consumer tenant or resident applicant prior to the procurement of the any consumer report or investigative consumer report by the End-User.

If the consumer's tenant application is denied, or other adverse action is taken based in whole or in part on the consumer reports provided by Company, End-User will provide to the consumer: (1) a notice of the adverse action, (2) the name, address, and telephone number of the consumer reporting agency that furnished the report and a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken, and (3) notice of the consumer's right to obtain a free copy of the consumer report from the consumer reporting agency that furnished the report within 60 days and of the consumer's right to dispute the accuracy or completeness of any information in the consumer report furnished by the consumer reporting agency. End-User certifies that any adverse action notice will comply with the FCRA including but not limited to satisfying all requirements under the FCRA if credit history is a disqualifying factor. If using a credit score, End-User certifies that it will comply with the Dodd-Frank Act and all applicable regulations relating to using a credit score.

k) Investigative Consumer Reports

In addition to the disclosure requirements identified above, if the consumer makes a written request for a complete and accurate disclosure of the nature and scope of the investigation requested within a reasonable amount of time after the consumer's receipt of disclosure, End-User will provide consumer with a complete and accurate written disclosure of the nature and scope of the investigation requested. End-User agrees to provide this information to the consumer no later than five (5) days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the later.

l) International Criminal Record Searches

End-User understands that searches of international background screening will be conducted through the services of a third-party independent contractor. Because of differences in foreign laws, language, and the way foreign records are maintained and reported, Company cannot be either an insurer or guarantor of the accuracy of the information reported. End-User therefore releases Company and its affiliated companies, officers, agents, employees, and independent contractors from any liability whatsoever in connection with erroneous information received because of an international background screening report.

m) National/Multi-State Database Searches

Company recommends that End-User screen its applicants or employees at the county court-house or online system, federal, and multi-state/nationwide database levels. End-User understands that if it chooses not to conduct searches at these levels, Company cannot be held responsible for any records that exist that are not included in the End-User's coverage requested. End-User further understands that the multi-state/nationwide database report will only be offered in conjunction with a county-level verification of any records found and that End-User will bear any additional costs associated with this verification.

n) Text Messaging (SMS) Service

If End-User requests the Company to communicate with consumers via text message to a phone number disclosed by the consumer, End-User understands that it is responsible for obtaining all necessary authorizations for compliance with the Telephone Consumer Protection Act ("TCPA") permitting the Company and its service providers to send text messages to the disclosed phone number. End-User certifies that it will only request the Company to communicate with consumers via text message only after End-User has obtained such authorization(s). End-User shall provide written evidence of opt-in upon request from Company and End-User agrees to notify Company immediately of the name and number of any consumers who have not opted-into or have opted-out of receiving SMS messaging.

End-User represents and warrants that End-User's use of the Services will not violate any applicable law or regulation. End-User further represents and warrants that End-User will only communicate with individuals in a manner that does not cause either the Company or the End-User to violate any applicable statute, rule, or regulation relating to the use of e-mail, telephonic calls, text

messages, SMS messages, “in-app” communications, or similar methods of communicating with individuals who may be the target of the Services obtained by the End-User.

o) Miscellaneous

End-User understands and agrees that access to certain types of information (e.g., credit, motor vehicle records, I-9 verification, etc.) may require End-User to execute a separate contract, agreement, or addendum (as applicable) with Company or with Company’s vendors or service providers. End-User understands that Company will not provide to End-User or allow End-User access to such information unless and until it executes the relevant contract(s), agreement(s) or addenda (as applicable).

4.Additional Requirements for Motor Vehicle Records (MVRs) and Driving Records

End-User hereby certifies that Motor Vehicle Records and/or Driving Records (MVRs) shall only be ordered in strict compliance with the Driver Privacy Protection Act (“DPPA”, at 18 U.S.C. § 2721 *et seq.*) and any related state laws. End-User further certifies that no MVRs shall be ordered without first obtaining the written consent of the consumer to obtain “driving records,” evidence of which shall be transmitted to Company in the form of the consumer’s signed release authorization form. End-User also certifies that it will use this information only in the normal course of business to obtain lawful information relating to the holder of a commercial driver’s license or to verify information provided by an applicant or employee. End-User shall not transmit any data contained in the resulting MVR via the public internet, electronic mail or any other unsecured means.

5.Warrants

In the course of completing background checks, Company may uncover active arrest warrants which are outstanding against the subject. In these cases, Company may be contacted by the law enforcement agency seeking the subject. End-User understands that Company will furnish to law enforcement any information contained within the subject’s file to assist in the apprehension of the subject. Additionally, Company may contact End-User, and End-User agrees to release to Company, all information End-User may have which will further the apprehension of the wanted individual.

6.General Provisions

a) End-User agrees not to resell, sub-license, deliver, display or otherwise distribute to any third party any of the consumer reports and investigative consumer reports addressed herein, except as required by law. End-User may not assign or transfer this Agreement without the prior written consent of Company. In addition, End-User shall immediately notify Company of any of the following events: change in ownership of End-User (over 50%), a merger, change in name or change End-user’s business. The parties understand that this Agreement is for the sole benefit of Company and End-User and no third party shall be deemed a third-party beneficiary of this Agreement. If any of the provisions of this Agreement become invalid, illegal, or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions shall not in any way be impacted. By agreement of the parties, IDAHO law shall guide the interpretation of this Agreement, if such interpretation is required. All litigation arising out of this Agreement shall be commenced in IDAHO**,** and the parties hereby consent to such jurisdiction and venue. Any written notice by either party shall be delivered personally by messenger, private mail courier service, or sent by registered or certified mail, return receipt requested, postage prepaid to the addresses listed below. This Agreement shall be construed as if it were jointly prepared. Both parties agree that this Agreement constitutes all conditions of service, present and future. Changes to these conditions may be made only by mutual written consent of an authorized representative of End- User and an officer of Company. The headings of each section shall have no effect upon the construction or interpretation of any part of this Agreement.

b) If End-User is permitted to request consumer reports for employment purposes via Company’s website, then, in addition to all other obligations, End-User agrees to abide by such additional conditions that may be imposed to utilize the website, provide all required certifications electronically, to maintain complete and accurate files containing all required consent, authorization and disclosure forms with regard to each consumer for whom a report has been requested, and maintain strict security procedures and controls to assure that its personnel are not able to use End-User’s Internet access to obtain reports for improper, illegal or unauthorized purposes. End-

User agrees to obtain the consumer's electronic consent to receive any legal or other notices electronically. End-User agrees to allow Company to audit its records at any time, upon reasonable notice given. Breaches of this Agreement and/or violations of applicable law discovered by Company may result in immediate suspension and/or termination of the account, legal action and/or referral to federal or state regulatory agencies.

c) Company requires criminal history background checks for any authorized user of End-User to determine whether the authorized user can be trusted to use the Services and information derived from the Services only for a legitimate business purpose and not disclose such information except as permitted by this Agreement and applicable law. As allowed by law, and subject to an individualized assessment, such background checks must not reveal any felony or misdemeanor conviction for the seven (7) years preceding the date that the employee of End-User gains access to the Verified First Background Screening Portal. End-User must retain each background check report for as long as an individual is an authorized user and for two years thereafter and will make such background check reports available for review by Company upon reasonable request.

d) End-User understands and agrees that if it fails to place any orders for consumer reports or investigative consumer reports for a period of thirteen (13) months, Company will automatically disable their account after which time End-User must complete a new application for services and undergo credentialing before its service is restored.

7.Monitoring Products

It is the sole responsibility of End-User, and End-User represents and warrants that it maintains reasonable procedures, to promptly notify Company of any personnel changes that are relevant to ensuring accuracy of the checks performed in connection with the monitoring products and appropriate access control, including but not limited to MVR, Healthcare Compliance and Criminal. In addition, End-User shall comply with all applicable federal, state and local laws in connection with use of the monitoring products, including but not limited to any additional consent requirements under California law.

8.Confidentiality

a) Neither party shall reveal, publish, or otherwise disclose any Confidential Information to any third party without the prior written consent of the other party. "Confidential Information" means all Proprietary Intellectual Property (defined below) or secret data; sales or pricing information relating to either party, its operations, employees, products, or services; and, all information relating to any customer, potential customer, Agent, and/or independent sales outlet. Either party may disclose Confidential Information in response to a valid order of a court or other governmental body or as may otherwise be required by law to be disclosed; provided that the disclosing party gives sufficient notice to the other party to enable the other party to take protective measures. The Parties agree to always keep this information confidential during the term of this Agreement and continuing for five years after receipt of any Confidential Information. Notwithstanding anything to the contrary herein, in no event shall Company be required to destroy, erase or return any consumer reports or applicant data related thereto in Company's files, all of which Company shall maintain as a consumer reporting agency in strict accordance with all applicable federal, state, and local laws.

b) In connection with Services, End-User may have access to Confidential Information relating to Company's intellectual property, including but not necessarily limited to trade secrets, service marks, trademarks, trade names, logos, symbols, brand names, software, technology, inventions, processes (that are subject to a patent or otherwise pending) collectively "Proprietary Intellectual Property." End-User acknowledges and agrees that Company is the sole exclusive owner of all right, title and interest in such Proprietary Intellectual Property and it shall not disclose to any third party the nature or details of any such Proprietary Intellectual Property. End- User further agrees that it has no right to publish, reproduce, prepare derivative works based upon, distribute, perform or otherwise display any of Company's Proprietary Intellectual Property.

9.Independent Contractor

The parties agree that the relationship of the parties created by this Agreement is that of independent contractor and not that of employer/employee, principal/agent, partnership, joint venture or representative of the other. Except as authorized hereunder, neither party shall represent to third parties that it is the employer, employee, principal, agent, joint venture or partner with, or representative of the other party.

10.Fees and Payment

a) End-User must provide ACH debit information or a valid credit card to Company before End-User can order any services. If End-User opts for credit card, the End-User agrees to pay up to 4% credit card processing fee, varied by applicable state law. End-User is solely responsible for ensuring that payment information is always complete and accurate.

b) End-User agrees to pay nonrefundable fees and other charges or costs for Company background check services. Any charges or costs, including but not limited to surcharges and other fees levied by federal, state, county, other governmental agencies, educational institutions, employer verification lines and licensing agencies, incurred by Company in servicing End-User, will be passed onto End-User. At Company's option, payments not received thirty (30) days after the date of the invoice may cause the account to be placed on temporary interruption, with no additional requests being processed until the balance due is paid in full or arrangements have been made with Company's Accounts Payable Department. Accounts with invoices unpaid thirty (30) days or more will be assessed an interest charge of 1.5 % per month, as allowed by applicable law. In addition, Company charges a 4% fee, or such other amount as permitted by applicable laws for collecting payments via credit card. Any concerns regarding invoices or line items must be brought to the attention of Company's billing department within 15 days of the date of such invoice. A $25 fee will be charged on all returned checks and non-sufficient funds.

c) If the account goes to collection, End-User agrees to pay all collection expenses, including attorneys' fees and court costs. End-User agrees that prices for services are subject to change without notice, although Company will make every reasonable effort to give notice of such change before it becomes effective. Any account that remains inactive for a period of twelve (12) months will be deemed inactive and may be terminated by Company.

11.Warranties, Remedies, and Limitation of Liability

a) End-User understands that Company obtains the information reported in its consumer reports from various third-party sources "AS IS", and therefore is providing the information to End-User "AS IS".

b) End-User represents and warrants that End-User's use of the Services will not violate any applicable law or regulation. End-User further represents and warrants that End-User will only communicate with individuals in a manner that does not cause either the Company or the End-User to violate any applicable statute, rule, or regulation relating to the use of e-mail, telephonic calls, text messages, SMS messages, "in-app" communications, or similar methods of communicating with individuals who may be the target of the Services obtained by the End-User.

c) Company makes no representation or warranty whatsoever, express or implied, including but not limited to, implied warranties of merchantability or fitness for particular purpose, or implied warranties arising from the course of dealing or a course of performance with respect to the accuracy, validity, or completeness of any consumer reports or investigative consumer reports, that the consumer reports or investigative consumer reports will meet End-User's needs, or will be provided on an uninterrupted basis; Company expressly disclaims any and all such representations and warranties.

d) End-User represents and warrants that it has developed, implemented, and continues to maintain a written information security program ("WISP") that includes administrative, technical, and physical safeguards designed to endure the confidentiality, integrity, and availability of data and systems used by End-User to obtain products and services provided by Company. End User further represents

and warrants that its WISP shall include safeguards which are consistent with and equivalent to the safeguards specified in Addendum A, attached hereto and incorporated by reference.

e) COMPANY WILL NOT BE LIABLE TO END-USER FOR DAMAGES, AND END-USER HEREBY RELEASES COMPANY FROM ANY LIABILITY FOR ANY AND ALL KINDS OF DAMAGES ARISING UNDER ANY THEORY OF LEGAL LIABILITY TO THE FULLEST EXTENT THAT END- USER MAY LEGALLY AGREE TO RELEASE COMPANY FROM LIABILITY FOR SUCH DAMAGES, NONETHELESS, IN THE EVENT COMPANY IS DETERMINED BY A COURT OF COMPETENT JURISDICTION TO BE LIABLE TO END-USER FOR ANY MATTER ARISING UNDER OR RELATING TO THIS AGREEMENT, WHETHER ARISING IN CONTRACT, EQUITY, TORT OR OTHERWISE (INCLUDING WITHOUT LIMITATION ANY CLAIM FOR NEGLIGENCE), THE AMOUNT OF DAMAGES RECOVERABLE AGAINST COMPANY FOR ALL SUCH MATTERS WILL NOT EXCEED, IN THE AGGREGATE, ***THE AMOUNT PAID TO COMPANY BY END-USER FOR THE SPECIFIC SERVICE TO WHICH A GIVEN CLAIM RELATES (BY WAY OF EXAMPLE ONLY, THE AMOUNT PAID BY END-USER FOR A PARTICULAR BACKGROUND REPORT AT ISSUE IN THE UNDERLYING CLAIM)***; RECOVERY OF THE FOREGOING IS END-USER'S SOLE AND EXCLUSIVE REMEDY HEREUNDER. IN THE EVENT COMPANY IS LIABLE TO END- USER FOR ANY MATTER RELATING TO THIS AGREEMENT, WHETHER ARISING IN CONTRACT, EQUITY OR TORT (INCLUDING WITHOUT LIMITATION ANY CLAIM FOR NEGLIGENCE), AND IN ADDITION TO ANY OTHER LIMITATION OF LIABILITY OR REMEDY SET FORTH IN THIS AGREEMENT, THE AMOUNT OF DAMAGES RECOVERABLE AGAINST COMPANY WILL NOT INCLUDE ANY AMOUNTS FOR INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, LOST INCOME, OR LOST SAVINGS, OR ANY OTHER INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES EVEN IF COMPANY HAS BEEN ADVISED OF THE POSSIBILITY FOR SUCH DAMAGES.

f) End-User shall indemnify, defend and hold harmless Company, its successors and assigns, officers, directors, employees, agents, vendors, credit bureaus and suppliers from and against any and all third-party claims, demands, suits, or proceedings, and any and all actual damages, costs, expenses (including, without limitation, reasonable attorneys' fees and court costs) ("Losses") arising or resulting from, or otherwise in connection with consumer reports and investigative consumer reports provided by Company, including but not limited to the content, compliance, method of delivery or effectiveness of any notices, pre-adverse or adverse action letters, including in the use of Company's applicant pay system or Company's facilitation of any consumer payments made in connection with consumer reports and investigative consumer reports provided by Company, any breach by End-User of any of its representations, warranties, or agreements in this Agreement or End-User's negligence or willful misconduct. Company shall have no responsibility for consequences of the actions of End-User upon the information which Company provides End-User, and End-User will indemnify and hold Company harmless from any loss, liability, damage, judgment, attorney's fees, costs, or penalties which may result from the use by End-User of the information provided by Company.

g) End-User agrees it is solely responsible for having adequate and legally compliant disclosures, adverse action letters, and processes under the FCRA and applicable state and local law. Company does not guarantee End-User's compliance with all applicable laws in its use of reported information, and does not provide legal or other compliance-related services upon which End-User may rely in connection with its furnishing of reports. End-User understands that any documents, sample forms and letters, information, conversations or communication with Company's representatives regarding searches, verifications or other services offered by Company are for information purposes only and not to be considered a legal opinion regarding such use. End-User agrees that

> (1) it will consult with its own legal or other counsel regarding the use of background screening information, including but not limited to, the legality of using or relying on reported information and to review any sample forms as well as the content of prescribed notices, sample adverse or pre-adverse action letters and any attachments to this Agreement for compliance with all applicable laws and regulations and (2) the provision and content of such notices, pre- adverse or adverse action letters and the contents thereof is the sole responsibility of End-User not Company. End-User acknowledges and agrees that it has no obligation to use and is solely responsible for independently vetting the contents of, any sample forms, disclosures, or letters that Company has provided to End-User in connection with this Agreement. Company fully disclaims any and all liability relating to the content, compliance or effectiveness of any such certifications, consumer consents,

forms, notices, summary of rights, disclosures, authorizations, pre-adverse or adverse action letters, other materials or information. If End-User utilizes Company's candidate entry system and/or its adverse action processing system, End-User agrees that it has had such processes, documents and letters reviewed by its counsel.

h) Company will keep information it provides to End-User in accordance with company's data retention policy, found at **https://legal.verifiedfirst.com/#/legal#data-retention-policy**

12.Term and Termination

a) The term of this Agreement shall begin on the date it is executed by End-User and shall be in effect for one (1) year beginning on the last date of signature below and renewed automatically for one (1) year each year on its anniversary date, if no written notice is received by either party within thirty (30) days prior to end of term.

b) Except as otherwise provided for herein, either party may cancel this Agreement by giving thirty (30) day written notice to the other party. If End-User desires to terminate this Agreement, End-User agrees that it will pay Company for all services that have been provided prior to the effective date of termination. Company may terminate or revise the provisions of this Agreement immediately upon written notice if End-User is the debtor in a bankruptcy action or in an assignment for the benefit of creditors or if End-User undergoes a change in ownership. Termination of this Agreement by either party does not release End-User from its obligation to pay for services rendered or other responsibilities and agreements made.

c) In addition to any and all other rights a party may have available according to law, if a party defaults by failing to perform any provision, term or condition of this Agreement the other party may terminate the Agreement by providing written notice to the defaulting party. This notice shall describe with sufficient detail the nature of the default. The party receiving such notice shall have fifteen (15) days from the receipt of such notice to cure the default(s). Unless waived by party providing notice, the failure to cure the default(s) within such time period shall result in the automatic termination of this Agreement.

13.Force Majeure

End-User agrees that Company is not responsible for any events or circumstances beyond its control (e.g., including but not limited to war, terrorism, riots, embargoes, strikes, internet or telecommunication failures, acts by hackers or other malicious third parties, and/or Acts of God or governmental action) that prevent Company from meeting its obligations under this Agreement and such performance, except for any payment obligations of End-User, shall be excused to the extent that it is prevented or delayed by reason of any of the foregoing.

14.Waiver

The failure of either party to insist in any one or more cases upon the strict performance of any term, covenant or condition of this Agreement will not be construed as a waiver or subsequent breach of the same or any other covenant, term or condition; nor shall any delay or omission by either party to seek a remedy for any breach of this Agreement be deemed a waiver by either party of its remedies or rights with respect to such a breach.

15.Severability

If any provision of this Agreement, or the application thereof to any person or circumstance, shall be held invalid or unenforceable under any applicable law, such invalidity or unenforceability shall not affect any other provision of this Agreement that can be given effect without the invalid or unenforceable provision, or the application of such provision to other persons or circumstances, and, to this end, the provisions hereof are severable.

16.Execution

This Agreement and all attachments, exhibits and addendums hereto, constitute the entire agreement of the parties and shall supersede any prior agreements governing the subject matter contained herein. Neither party will be bound by, and each specifically objects to, any provision that is different from or in addition to this Agreement (whether proffered verbally or otherwise), unless such provision is specifically agreed to in writing and signed by both parties. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. A signature on a copy of this Agreement received by either party by facsimile is binding upon the other party as an original. The parties shall treat a photocopy of such facsimile as a duplicate original. The individuals signing below represent that they are duly authorized to do so.

Signature

I certify that I am authorized to execute this Agreement on behalf of the company listed below. Further, I certify on behalf of such company, that the above statements are true and correct and agree for the company to the terms and conditions set forth in the Agreement.

On Behalf of End-User:

Company Name:

Company Address:

Date:

Print Name:

Title:

Signature:

Who is going to be your primary user with full administrative rights?

Name:

Direct Phone:

Email:

I understand the pricing being offered is based off an average monthly volume of 20 orders placed. End-User Company is registered with the Secretary of State in the State of:
We plan to place our first order on or before:

On Behalf of Verified First, LLC

Name:

Title:

Date:

Signature:

ADDENDUM A

Access Security Requirements

1.Access Control Measures

1.1. Policies, procedures, and physical and technical controls: (i) to limit physical access to its file storage, information systems, and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Confidential Information, especially PI, have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Confidential Information or information relating thereto to unauthorized individuals; and (iv) to encrypt and decrypt PI and other relevant Confidential Information where appropriate.

1.2. All of End-User's employees and agents shall take reasonable steps to protect their usernames, account numbers and passwords such that only key personnel employed by End-User with a need to have access to the Confidential Information will have such access. End-User agrees to notify Company and change account passwords immediately if a person with an assigned password leaves the End-User's employment or no longer needs to have system access due to a change in duties.

2.Security Awareness and Training.

2.1. A security awareness and training program for all members of End-User's workforce (including management), which includes training on how to implement and comply with its security controls. At a minimum, such awareness and training program shall adhere to the following:

(a) Annual training regarding Applicable Privacy Laws for all personnel who process Personal Information; and

(b) Annual training regarding functionally specific data protection controls which apply to each End-User worker's job function where such worker processes Personal Information.

3.Security Incident Procedures.

Policies and procedures to detect, respond to, and otherwise address security incidents, unusual or suspicious events and similar incidents including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into PI or Confidential Information or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes as well as to permit identification and prosecution of violators.

4.Contingency Planning.

Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Confidential Information or systems that contain Confidential Information, including a data backup plan and a disaster recovery plan.

5.Device and Media Controls.

Policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential Information into and out of a End-User facility, and the movement of these items within a End-User facility, including policies and procedures to address the final disposition of Confidential Information, and/or the hardware or electronic media on which it is stored, and procedures for removal of Confidential Information from electronic media before the media are made available for re-use.

6.Audit Controls.

6.1. End-User shall properly implement, maintain and enforce privacy and data security policies and, if requested by Company, promptly provide to Company copies of all such policies relevant to the Processing of Personal Information for Company to review.

6.2. End-User shall reasonably cooperate with Company, at Company's expense, in connection with any Company or governmental investigations regarding Company Personal Information or the provision of the Services.

6.3. Upon reasonable advance notice to End-User and during normal business hours, Company may conduct a security audit of End-User's facilities, at Company's expense, by representatives of Company, including without limitation its independent third-party auditor, provided that:

(a) such security audit shall occur at a mutually agreeable time not more than once during any given calendar year; provided, however, that Company shall have the right (i) to conduct an additional security audit in response to each Security Incident; and (ii) to conduct follow-up security audits.

(b) such site visit shall not unreasonably interfere with End-User's operations; and

(c) any third party performing such site visit on behalf of Company shall execute a nondisclosure agreement with End-User in a form acceptable to End-User with respect to the confidential treatment and restricted use of End-User's confidential information.

7.Data Integrity.

7.1. Policies and procedures to ensure the confidentiality, integrity, and availability of Confidential Information and protect it from disclosure, improper alteration, or destruction.

7.2. End-User shall keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates. End-User shall configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best commercial security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

7.3. End-User shall implement and follow current best commercial security practices for Computer Virus detection scanning services and procedures by adhering to the following:

(a) End-User shall use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.

(b) If End-User suspects an actual or potential virus, End-User shall immediately cease accessing the system and shall not resume use of the system until the virus has been eliminated.

(c) On a commercially reasonable, regular weekly basis at a minimum, End-User shall keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files. If End-User's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-virus scans be completed more frequently than weekly.

(d) End-User shall implement and follow current best commercial security practices for computer anti-Spyware scanning services and procedures by adhering to the following:

(i) Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.

(ii) If End-User suspects actual or potential Spyware, immediately cease using the system and do not resume use until the problem has been resolved and eliminated.

(iii) Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from End-User's computers.

(iv) Keep anti-Spyware software up-to-date by vigilantly checking or configuring updates and installing new anti-Spyware definition files on a commercially reasonable, regular basis weekly, at a minimum. If End-User's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

8.Storage and Transmission Security.

8.1. Technical security measures to guard against unauthorized access to Confidential Information that is being transmitted over an electronic communications network, including a mechanism to encrypt electronic information whenever appropriate, such as while in transit or in storage on networks or systems to which unauthorized individuals may have access.

8.2. End-User shall develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)

8.3. End-User shall protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best commercial security practices. Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.

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

8.5. End-User shall disable outside vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

9.Secure Disposal.

9.1. Policies and procedures regarding the disposal of Confidential Information, and tangible property containing Confidential Information, taking into account available technology so that Confidential Information cannot be practicably read or reconstructed.

9.2. In accordance with the FACTA Disposal Rules, End-User shall implement appropriate measures to dispose of any sensitive information related to consumer reports and records, including the Confidential Information, that will protect against unauthorized access or use of that information.

10. Assigned Security Responsibility.

End-User shall designate a security official responsible for the development, implementation, and maintenance of its WISP. End-User shall inform Company as to the person responsible for security.

11.Testing.

11.1. End-User shall regularly and no less than one time per year test the key controls, systems and procedures of its WISP to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

11.2. End-User shall use current best commercial practices to protect its telecommunications systems and any computer system or network device(s) to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

(a) protecting against intrusions;

(b) securing the computer systems and network devices; and

(c) protecting against intrusions of operating systems or software.

12.Adjust the Program.

End-User shall monitor, evaluate, and adjust, as appropriate, the WISP in light of any relevant changes in technology or industry security standards, the sensitivity of the Confidential Information, internal or external threats to End-User or the Confidential Information, requirements of applicable work orders, and End-User's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

ADDENDUM B

Documents Required Before Requesting Credit Report Information

Before End-User will be allowed to access credit report information or employment verification data obtained from TALX (an Equifax Company), Company requires that End-User provide one (1) of the following items listed below (if End-User is not publicly traded) and also receive an onsite inspection to verify company information and physically review End-User's onsite location. Certain criteria must be met at the onsite inspection per requirements of the credit bureau. Cost for the onsite inspection will be the responsibility of the End- User and End-User will receive an invoice for any related costs and expenses from Verified First.

1. Business license status from a government web site (please include entire web page print out);
2. Business license, copy or documented verification.
3. Documented corporation verification with state or federal government.
4. Copy of Articles of Incorporation with proof of filing.
5. State and/or federal tax records originating from the state or federal government.
6. FDIC Certification; or
7. 501(c)(3) certificate for non-profit organizations.

If End-User is a publicly traded company, the following items are acceptable methods for verifying that the End-User is a bona fide entity:

1. Documentation of ticker symbol information from trading website.
2. Certified copy of audited annual or quarterly statements submitted to the SEC.