

## Justifacts Credential Verification, Inc Credential Verification Service Agreement

This Credential Verification Service Agreement ("Agreement") is entered into and effective as of June 1, 2018 ("Effective Date"), by and between Justifacts Credential Verification, Inc. ("Justifacts"), a Pennsylvania Corporation with offices at 5250 Logan Ferry Road, Murrysville PA 15668 and City of Grand Junction ("Client").

**WHEREAS**, Justifacts has certain specialized knowledge, experience and skills related to pre-employment background investigation/credential verification (herein after Verification Services); and

**WHEREAS**, Client desires to receive such Verification Services in accordance with the terms and conditions set forth in this Agreement;

**NOW THEREFORE**, in consideration of the agreements and covenants set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

### 1. OBLIGATIONS OF JUSTIFACTS.

**1.1 Compliance with law.** During the term of this Agreement, Justifacts will provide Verification Services in accordance with the Fair Credit Reporting Act ("FCRA") and any applicable state laws. The Verification Services include all activities related to the creation of a consumer report or investigative consumer report, as defined in section 603 of the FCRA, concerning certain individuals who:

- a. Have applied for employment with the Client or who are currently employed by the Client; or
- b. Have entered into a business transaction with Client; or
- c. Have given written instructions specifying the purpose for obtaining a consumer report.

**1.2 Service Initiation.** Justifacts agrees to perform Verification Services for the Client upon receipt of a properly executed Credential Verification Service Agreement as well as an executed Agreement to Abide by the Fair Credit Reporting Act (Exhibit A). The Verification Services will be initiated by the Client via order entry into Justifacts online Internet based website, Justiweb, or via an integrated and secure connection between Justifacts and Client. Justifacts will only perform those services specifically requested by the Client.

**1.3 Product Produced.** Justifacts will electronically return a completed Background Screening Report ("Report") detailing the results of the requested Verification Service(s) to the Client via the online Internet based system, Justiweb, or via an integrated and secure connection between Justifacts and Client.

**1.4 Customer Support.** Justifacts will provide Client with all levels of customer support, consistent with industry standards. Customer Service will be provided via live online chat,

inbound live telephone calls, inbound mail, inbound email and inbound fax during normal business hours, currently between 8:00 am Eastern time and 8:00 pm Eastern Time.

**1.5 Data Security and Privacy.** Justifacts shall maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate for the nature and scope of its activities, and the sensitivity of the information provided to Justifacts by Client; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Client, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. At minimum, Justifacts shall comply with the Access Security Requirements set forth in Exhibit "B". Justifacts is not responsible for any disclosure or compromise of such data due to Clients acts or omissions or resulting from use of Clients logins and passwords, due to no fault of Justifacts.

**1.6 Record keeping.** During the term of this Agreement, Justifacts shall maintain Reports on the Justifacts system for a minimum of seven (7) years in the active Justweb database, and eight (8) to ten (10) years of data will be stored on cold storage. Following the expiration or termination of this Agreement, Justifacts will provide a reasonable opportunity to allow Client to: (i) download copies of any Reports, and/or (ii) obtain from Justifacts, at Justifacts then current fee, a disc or other similar media containing copies of Reports. After ten (10) years, Justifacts shall have no further duty to maintain copies of Reports for access by Client.

## 2. OBLIGATIONS OF CLIENT.

**2.1 Exclusive Use.** Client agrees that the information will be requested for Client's exclusive use and shall not be resold. All consumer information will be held in strict confidence, except as permitted by law. Reports on applicants or employees will be requested only by Client's designated representatives, identified in writing to Justifacts by Client. Employees of Client shall be forbidden to attempt to obtain reports on themselves, associates, or any other person except in the exercise of their official duties.

**2.2 FCRA Compliance.** Client will complete the Justifacts Agreement to Abide by the Fair Credit Reporting Act ("Exhibit A") and acknowledges that they have received the following notices prescribed by the FCRA: (1) Notice to Users of Consumer Reports; (2) A Summary of Your Rights under the FCRA; and (3) Remediating the Effects of Identity Theft.

**2.3 GLB Act Compliance.** The federal Gramm-Leach Bliley Act, 15 U.S.C.A. Section 6801 et.seq (2000), ("GLB Act") was enacted to protect the use and disclosure of non-public personal information, including, in certain instances, the use of identifying information only. Client agrees that it will comply with all GLB Act requirements as they apply to information provided by Justifacts and shall restrict the use of such information for employment or background screening purposes only.

**2.4 Data Security and Privacy.** Client shall maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to Client size and

complexity, the nature and scope of its activities, and the sensitivity of the information provided to Client by Justifacts; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Justifacts, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. At minimum, Client shall comply with the Access Security Requirements set forth in Exhibit "B".

**2.5 Legal counsel/advice.** Client agrees that Justifacts is not engaged to provide legal advice and that it is incumbent upon the Client to engage its own legal counsel to ensure that they are in compliance with all requirements of the FCRA as well as all other applicable state and federal laws. Client acknowledges that Justifacts does not offer opinions on report content and that Client shall base its screening process on its own background screening policy. Any forms provided by Justifacts are for informational purposes only and not for the purpose of providing legal advice. Justifacts recommends that Client have all forms reviewed by legal counsel to determine the suitability for Clients specific situation.

**2.6 Record keeping.** Because of the unique nature of the Verification Services provided by Justifacts and requirements placed on Justifacts in obtaining information according to federal and state law and third-party contractual obligations, Justifacts may perform periodic audits or be required to supply verification that Client is in compliance with this Agreement. Except for those documents hosted on Justifacts system, Client agrees to maintain in its records a copy of all consent forms, disclosures and pre-adverse and adverse action notices for a minimum of 5 years and Client shall, upon reasonable notice, provide Justifacts or its designated representatives such documents to show compliance with its obligations in this Agreement.

**2.7 Account Access.** Client shall designate a primary contact (Contact) for the Justifacts account who shall be responsible for the administration and control of Clients account. The Contact shall identify and authorize all Client users and their level of access to the Justifacts system and will promptly notify Justifacts of any changes to users or access privileges.

- 3. FEES.** Client agrees to pay Justifacts for providing Verification Services according to the Fee Schedule set forth in Exhibit "C". If Client requests additional services not initially set forth in the Fee Schedule, such added services will be hereby incorporated into this Agreement at Justifacts then-current rate unless otherwise mutually agreed-upon in writing by the parties. Client acknowledges that it will be responsible for charges resulting from its data input errors, duplicate requests and request cancellations initiated after processing has commenced. Client shall pay all pass-through fees incurred from information sources (including but not limited to The Work#, National Student Clearinghouse, DMV, courts, etc) for release of information or records used in compiling the Verification Services. Such pass-through fees are subject to change without prior notice. If at any time there are any changes in laws or government regulations that increase Justifacts cost to provide services or reasonably requires additional services to be provided by Justifacts, or in Justifacts determination restrict its ability to reasonably continue to provide the service(s) in this Agreement, Justifacts may, upon providing prior written notice to Client: (i) add a reasonable fee or pricing change to cover the added costs of providing the affected service(s), and/or (ii) modify or cease providing the affected service(s). Justifacts will

conduct annual audits of Client account to determine order history, number of reports requested and criminal hit ratio (Number of reports with a criminal record/total number of criminal record reports requested). If the volume of requests does not meet anticipated levels, Justifacts may, upon providing 30-day prior written notice to Client, increase the cost of services provided to meet the actual volume of report requests. If the hit ratio for criminal records exceeds 25%, Justifacts may, upon providing 30-day prior written notice to Client, increase the cost of criminal record search requests to meet the higher rate of criminal records found.

4. **PAYMENTS.** Justifacts shall invoice Client on a monthly basis and Client will promptly review each invoice and notify Justifacts of any errors or disputes on or before the due date of such invoice. Within thirty (30) days of the date of an invoice from Justifacts, Client will submit payment for all undisputed amounts. If all undisputed amounts are not received by Justifacts by the due date, Justifacts may: (i) suspend Client's account until all delinquent payments are received, and/or (ii) charge Client a finance charge of 1½% per month or a minimum of \$1, whichever is greater, and/or (iii) charge a late fee of \$15 for all undisputed amounts outstanding over 60 days. In the event of a dispute regarding fees or charges, the parties will use reasonable efforts to discuss in good faith and come to an agreement regarding resolution of such dispute. All amounts to be paid herein will be in U.S. Dollars.

## 5. TERM AND TERMINATION.

**5.1 Term.** The term of this Agreement will be one (1) year from the date of this Agreement unless otherwise terminated as provided herein. The term of this Agreement shall automatically renew on a month-to-month basis until either party terminates the agreement by giving the other party not less than thirty (30) days written notice of termination before the end of the then current term.

**5.2 Material Breach.** For the purposes of this Agreement, Justifacts will be deemed to be in material breach of this agreement in that event that; (i) there are consistent or repeated material errors or inaccuracies with regard to the Verification Services provided by Justifacts of which Justifacts has prior notice from Client, and for which an opportunity to cure was provided; or (ii) Client receives repeated complaints from Client Representatives regarding the Verification Services, Justifacts has notice of such complaints and such complaints are not resolved to the satisfaction of Client. For the purposes of this agreement, Client will be in material breach of this agreement in the event that (i) its determined that Client is not in compliance with any federal or state law concerning the request, use or dissemination of information contained in the consumer reports provided by Justifacts, (ii) information is being requested by Client users on themselves or on individuals who have not properly authorized the collection or use of the information (iii) information is being resold or (iv) Client fails to pay invoice within the agreed payment terms. If either party is deemed to be in material breach, the non-breaching party may terminate this Agreement immediately upon written notice that the material breach remains uncured fifteen (15) days after the breaching party's receipt of the written notice of the breach pursuant to Section 5.3 (i) below.

**5.3 Termination.** This Agreement may be terminated by the parties as follows: (i) Either party may terminate this Agreement at any time in the event of a material breach by the other party of any provision of this Agreement that remains uncured fifteen (15) days after the breaching party's receipt of written notice of the breach; (ii) Either party may terminate this Agreement immediately if the other party becomes insolvent, or is unable to pay its debts or perform its obligations when due, or enters into or files (or has filed or commenced against it) a petition, arrangement, action or other proceeding seeking relief or protection under the bankruptcy laws of the United States or similar laws of the United States or any state of the United States or transfers all of its assets to another person or entity.

6. **WARRANTY.** Each party warrants and represents to the other party that it has full power and authority to enter into this Agreement and to carry out its obligations hereunder. Justifacts warrants to Client that (i) Justifacts has the authority to perform the Verification Services; (ii) during the term of this Agreement, Justifacts will comply with all laws applicable to the performance of the Verification Services as well as preparation, content, licensing, distribution and transmission of the products or services offered for sale on the Justifacts website in each jurisdiction where such compliance by Justifacts is necessary. Client warrants to Justifacts during the term of this Agreement, Client will comply with all laws applicable to the Client in respect to the preparation, content, licensing, distribution and transmission and use of the Verification Services provided by Justifacts.
  
7. **INDEMNITY.** Client agrees to defend, indemnify and hold Justifacts harmless from any and all liabilities, damages, claims, and cost of defense or actions arising out of any claim (a) relating to the performance or breach of Client's obligations or responsibilities under this Agreement; (b) relating to the preparation, submission, dissemination or any information contained in a report under dispute by a consumer, provided that Justifacts promptly notifies Client of the consumer dispute and Client takes any adverse action against the consumer prior to receiving notification of the resolution of same from Justifacts. This indemnification and hold harmless provision will extend to damages, costs, and the expense of defending any claim against Justifacts. Justifacts will promptly notify Client of any suit or threat of suit that may obligate Client to indemnify Justifacts under the above provisions and be given reasonable opportunity to defend same. Justifacts will reasonably cooperate with Client with regard to the defense of any suit or threatened suit and Client will have authority to settle, pay or otherwise dispose of any such suit or threatened suit, subject to the approval of Justifacts, which approval will not be unreasonably withheld.

Justifacts agrees to defend, indemnify and hold Client harmless from any and all liabilities, damages, claims, and cost of defense or actions arising out of any claim (a) relating to the performance or breach of Justifacts obligations or responsibilities under this Agreement. This indemnification and hold harmless provision will extend to damages, costs, and the expense of defending any claim against Client. Client will promptly notify Justifacts of any suit or threat of suit that may obligate Justifacts to indemnify Client under the above provisions and be given reasonable opportunity to defend same. Client will reasonably cooperate with Justifacts with regard to the defense of any suit or threatened suit and Justifacts will have authority to settle, pay or otherwise dispose of any such suit or threatened suit, subject to the approval of Client, which approval will not be unreasonably withheld.

8. **WARRANTY DISCLAIMER.** EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER PARTY MAKES, AND EACH PARTY SPECIFICALLY DISCLAIMS, ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE, AND IMPLIED WARRANTIES ARISING FROM COURSE OF DEALING OR PERFORMANCE.

9. **LIMITATION OF LIABILITY.** EXCEPT WITH RESPECT TO (I) EACH PARTY'S INDEMNITY OBLIGATIONS HEREUNDER, (II) BREACHES OF CONFIDENTIALITY OBLIGATIONS UNDER SECTION 10, AND (III) ACTS OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND WHETHER OR NOT SUCH DAMAGES WERE FORESEEABLE, AND WHETHER OR NOT THAT PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 10. CONFIDENTIALITY.

**10.1 Confidential Information.** "Confidential Information" will mean and refer to information about the disclosing party's (or its suppliers) business or activities that is proprietary and confidential including but not limited to: (i) any and all information relating to the consumer reports created at the request of Client; (ii) any and all information contained in any usage reports or related to all terms and conditions of this Agreement and all attachments hereto; (iii) all business, financial, technical and other information of a party marked or designated by such party as "*confidential*" or "*proprietary*"; or (iv) information which, by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as confidential.

**10.2 Exclusions.** Confidential Information will not include information that (i) is in or enters the public domain without breach of this Agreement, (ii) the receiving party lawfully receives from a third party without restriction on disclosure and without breach of a nondisclosure obligation or (iii) the receiving party knew prior to receiving such information from the disclosing party or (iv) the receiving party develops independently of the other party's Confidential Information.

**10.3 Use and Disclosure Restrictions.** Each party agrees (i) that it will not disclose to any third-party or use any Confidential Information disclosed to it by the other except as expressly permitted in this Agreement and (ii) that it will take all reasonable measures to maintain the confidentiality of all Confidential Information of the other party in its possession or control, which will in no event be less than a reasonable degree of care. Notwithstanding the foregoing, each party may disclose Confidential Information (i) to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required by law or (ii) on a "need-to-know" basis under an obligation of

confidentiality to its legal counsel, accountants, banks and other financing sources and their advisors or (iii) to the extent needed to complete the requested Verification Services.

## 11. GENERAL.

**11.1 Modification.** Any amendment, modification, supplement, or other change to any provision of this Agreement must be in writing and signed by both parties. All amendments or modifications of this Agreement will be binding upon the parties despite any lack of consideration so long as such amendments or modifications are in writing and executed by the parties.

**11.2 Waiver.** All waivers must be in a writing signed by the waiving party. The failure of either party to insist upon strict performance of any provision of this Agreement, or to exercise any right provided in this Agreement, will not be considered a waiver for the future exercise of such provision or right. No waiver of any provision or right will affect the right of the waiving party to enforce any other provision or right in this Agreement.

**11.3 Independent Parties.** The parties to this Agreement are independent parties and nothing herein will be construed as creating an employment, agency, joint venture or partnership relationship between the parties. Neither party will have any right, power or authority to enter into any agreement for or on behalf of, or incur any obligation or liability, or to otherwise bind, the other party.

**11.4 No Assignment.** Neither party may assign their obligations or rights under this Agreement without the other party's written consent, provided that either party may assign this Agreement without the other's consent to a successor in interest in the event of a reorganization, merger, consolidation, or sale of all or substantially all of its assets.

**11.5 Compliance with Laws.** Each party will comply with all laws, rules, and regulations of the United States. This Agreement is in the English language only, which language will be controlling in all respects, and all versions of this Agreement in any other language will be for accommodation only and will not be binding upon the parties hereto. All communications and notices to be made or given pursuant to this Agreement will be in the English language.

**11.6 Jurisdiction.** The Agreement will be governed by the internal laws of the state of Pennsylvania without regard to conflict of laws provisions. Client hereby irrevocably consents to the personal jurisdiction of the federal and state courts sitting in Allegheny County in the State of Pennsylvania, and to service of process within or without Pennsylvania. Client further agrees that any court action relating to the enforcement of any judgment or seeking injunctive or other equitable relief will be brought in such courts.

**11.7 Construction.** Except as specifically provided in this Agreement, all notices required hereunder will be in writing and will be effective when received. This Agreement, including any exhibits attached hereto, constitutes the entire understanding and agreement with respect to its subject matter, and supersedes any and all prior or contemporaneous representations, understandings and agreements whether oral or written between the parties relating to the subject matter of this Agreement. In the event that any provision of this Agreement is found to be invalid or unenforceable pursuant to judicial decree or decision,

the remainder of this Agreement will remain valid and enforceable according to its terms. The section and paragraph headings used in this Agreement are inserted for convenience only and will not affect the meaning or interpretation of this Agreement.

The parties have duly executed this Agreement by the authorized signatures below.

Client:	<u>CITY OF GRAND JUNCTION</u>	Justifacts Credential Verification, Inc.
By:	<u><i>Claudia Hazelhurst</i></u>	By: <u><i>Andrew Yober</i></u>
Name:	<u>CLAUDIA HAZELHURST</u>	Name: <u>Andrew Yober</u>
Title:	<u>HUMAN RESOURCES DIRECTOR</u>	Title: <u>VP - Criminal Records</u>
E-Mail:	<u>CLAUDIAH@GJ.CITY.ORG</u>	Date: <u>06/21/18</u>
Date:	<u>JUNE 4, 2018</u>	



## Exhibit A - AGREEMENT TO ABIDE BY THE FAIR CREDIT REPORTING ACT

Client certifies and agrees:

That it will comply with the Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (hereinafter FCRA) and all other applicable statutes, both state and federal.

That each request for a consumer report or an investigative consumer report is being obtained for the following purposes and for no other purpose:

- (A) for employment purposes
- (B) in connection with a business transaction involving the consumer, which is:  
\_\_\_\_\_
- (C) In accordance with the written instructions of the consumer

That information will be requested only for the Client's exclusive use and will not be otherwise distributed or sold. Client shall use each Consumer Report only for one time use and shall hold the report in strict confidence, except to the extent permitted by law. Reports on employees will be requested only by Client's designated representatives. Client users are forbidden to attempt to obtain reports on themselves, associates, or any other person except in the exercise of their official duties.

That each time a request for a consumer report and/or a investigative consumer report is made of Justifacts for employment purposes, Client will comply with §604(b) and §606(a) of the FCRA and that each time a request for an investigative consumer report is made of Justifacts for any non-employment purpose, Client will comply with §606(a) of the FCRA:

§604(b): (1) the consumer has been given a clear and conspicuous written disclosure, in advance (in a document that consists solely of the disclosure), that a consumer report may be requested for employment purposes; (2) the consumer has authorized the Client, in writing, to procure the report; (3) the information in the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation as well as any law providing consumer credit or consumer identity protection; (4) before taking adverse action, based in whole or in part on the report, Client will: (a) provide the consumer a copy of the report and a copy of "The Summary of Your Rights under the FCRA"; (b) allow the consumer a designated period of time to contact Justifacts if the consumer wishes to dispute any information in the consumer report; (c) provide the Justifacts contact information; and (d) provide a final adverse action notice to the consumer if a final adverse employment decision is made.

§606(a): (1) provide the consumer with a clear and accurate written disclosure, no later than three days after the report is requested, that a report may be made including information as to their character, general reputation, personal characteristics and mode of living; (2) provide the consumer a copy of the "Summary of Your Rights under the FCRA"; (3) provide a statement that the consumer has the right to request additional disclosures and to provide these disclosures when requested by the consumer.

That Client has received the following notices prescribed by the FCRA: (1) Notice to Users of Consumer Reports; (2) A Summary of Your Rights under the FCRA; and (3) Remedying the Effects of Identity Theft. It is incumbent upon the client to engage its own legal counsel to ensure that they are in compliance with all requirements of the FCRA as well as all state and federal employment law.

The individual whose signature appears below represents that they are authorized to enter into this agreement on behalf of the Client.

**CLIENT**

Company: CITY OF GRAND JUNCTION

Signature: *Claudia Hazelhurst*

Print Name: CLAUDIA HAZELHURST

Title: HUMAN RESOURCES DIRECTOR

Date: JUNE 4, 2018

**ACCEPTED BY**

Justifacts Credential Verification, Inc.

Signature: *Andrew Yoder*

Print Name: Andrew Yoder

Title: VP - Credential Records

Date: 06/21/18

## Exhibit B - Access Security Requirements

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is Clients responsibility to implement these controls. Justifacts reserves the right to make changes to the Access Security Requirements without notification.

Client understands that the access security requirements are comprehensive and that some requirements may not apply if reports are being stored on Justifacts system only and not electronically stored by me. In accessing the services provided by Justifacts, Client agrees to follow these security requirements:

### 1. Implement Strong Access Control Measures

- 1.1 Do not provide your account Access Codes or passwords to anyone. No one from Justifacts will ever contact you and request your Access Codes or password.
- 1.2 Proprietary or third party system access software must have Access Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Access Code / password be changed immediately when:
  - Any system access software is replaced by system access software or is no longer used;
  - The hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect Justifacts Access Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Access Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
  - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to Justifacts information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to Justifacts information.
- 1.12 Ensure that personnel who are authorized access to Justifacts information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your client application.
- 1.13 Ensure that you and your employees do not access your own background/credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a business transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access Justifacts information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- 1.15 After normal business hours, turn off and lock all devices or systems used to access Justifacts reporting systems and information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain background reporting and credit information.

## 2. Maintain a Vulnerability Management Program

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 2.2 Configure Infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best 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.
- 2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
  - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
  - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
  - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
  - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
  - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
  - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
  - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company'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.

## 3. Protect Data

- 3.1 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.)
- 3.2 All Justifacts background reporting and credit data is classified as Confidential and must be secured to this requirement at a minimum.
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all Justifacts reports and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

## 4. Maintain an Information Security Policy

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

# Justifacts Credential Verification, Inc Credential Verification Service Agreement

This Credential Verification Service Agreement ("Agreement") is entered into and effective as of June 1, 2018 ("Effective Date"), by and between **Justifacts Credential Verification, Inc.** ("Justifacts"), a Pennsylvania Corporation with offices at 5250 Logan Ferry Road, Murrysville PA 15668 and City of Grand Junction ("Client").

**WHEREAS**, Justifacts has certain specialized knowledge, experience and skills related to pre-employment background investigation/credential verification (herein after Verification Services); and

**WHEREAS**, Client desires to receive such Verification Services in accordance with the terms and conditions set forth in this Agreement;

**NOW THEREFORE**, in consideration of the agreements and covenants set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

## 1. OBLIGATIONS OF JUSTIFACTS.

**1.1 Compliance with law.** During the term of this Agreement, Justifacts will provide Verification Services in accordance with the Fair Credit Reporting Act ("FCRA") and any applicable state laws. The Verification Services include all activities related to the creation of a consumer report or investigative consumer report, as defined in section 603 of the FCRA, concerning certain individuals who:

- a. Have applied for employment with the Client or who are currently employed by the Client; or
- b. Have entered into a business transaction with Client; or
- c. Have given written instructions specifying the purpose for obtaining a consumer report.

**1.2 Service Initiation.** Justifacts agrees to perform Verification Services for the Client upon receipt of a properly executed Credential Verification Service Agreement as well as an executed Agreement to Abide by the Fair Credit Reporting Act (Exhibit A). The Verification Services will be initiated by the Client via order entry into Justifacts online Internet based website, Justiweb, or via an integrated and secure connection between Justifacts and Client. Justifacts will only perform those services specifically requested by the Client.

**1.3 Product Produced.** Justifacts will electronically return a completed Background Screening Report ("Report") detailing the results of the requested Verification Service(s) to the Client via the online Internet based system, Justiweb, or via an integrated and secure connection between Justifacts and Client.

**1.4 Customer Support.** Justifacts will provide Client with all levels of customer support, consistent with industry standards. Customer Service will be provided via live online chat,

inbound live telephone calls, inbound mail, inbound email and inbound fax during normal business hours, currently between 8:00 am Eastern time and 8:00 pm Eastern Time.

**1.5 Data Security and Privacy.** Justifacts shall maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate for the nature and scope of its activities, and the sensitivity of the information provided to Justifacts by Client; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Client, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. At minimum, Justifacts shall comply with the Access Security Requirements set forth in Exhibit "B". Justifacts is not responsible for any disclosure or compromise of such data due to Clients acts or omissions or resulting from use of Clients logins and passwords, due to no fault of Justifacts.

**1.6 Record keeping.** During the term of this Agreement, Justifacts shall maintain Reports on the Justifacts system for a minimum of seven (7) years in the active Justweb database, and eight (8) to ten (10) years of data will be stored on cold storage. Following the expiration or termination of this Agreement, Justifacts will provide a reasonable opportunity to allow Client to: (i) download copies of any Reports, and/or (ii) obtain from Justifacts, at Justifacts then current fee, a disc or other similar media containing copies of Reports. After ten (10) years, Justifacts shall have no further duty to maintain copies of Reports for access by Client.

## 2. OBLIGATIONS OF CLIENT.

**2.1 Exclusive Use.** Client agrees that the information will be requested for Client's exclusive use and shall not be resold. All consumer information will be held in strict confidence, except as permitted by law. Reports on applicants or employees will be requested only by Client's designated representatives, identified in writing to Justifacts by Client. Employees of Client shall be forbidden to attempt to obtain reports on themselves, associates, or any other person except in the exercise of their official duties.

**2.2 FCRA Compliance.** Client will complete the Justifacts Agreement to Abide by the Fair Credit Reporting Act ("Exhibit A") and acknowledges that they have received the following notices prescribed by the FCRA: (1) Notice to Users of Consumer Reports; (2) A Summary of Your Rights under the FCRA; and (3) Remediating the Effects of Identity Theft.

**2.3 GLB Act Compliance.** The federal Gramm-Leach Bliley Act, 15 U.S.C.A. Section 6801 et seq (2000), ("GLB Act") was enacted to protect the use and disclosure of non-public personal information, including, in certain instances, the use of identifying information only. Client agrees that it will comply with all GLB Act requirements as they apply to information provided by Justifacts and shall restrict the use of such information for employment or background screening purposes only.

**2.4 Data Security and Privacy.** Client shall maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to Client size and

complexity, the nature and scope of its activities, and the sensitivity of the information provided to Client by Justifacts; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Justifacts, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. At minimum, Client shall comply with the Access Security Requirements set forth in Exhibit "B".

**2.5 Legal counsel/advice.** Client agrees that Justifacts is not engaged to provide legal advice and that it is incumbent upon the Client to engage its own legal counsel to ensure that they are in compliance with all requirements of the FCRA as well as all other applicable state and federal laws. Client acknowledges that Justifacts does not offer opinions on report content and that Client shall base its screening process on its own background screening policy. Any forms provided by Justifacts are for informational purposes only and not for the purpose of providing legal advice. Justifacts recommends that Client have all forms reviewed by legal counsel to determine the suitability for Client's specific situation.

**2.6 Record keeping.** Because of the unique nature of the Verification Services provided by Justifacts and requirements placed on Justifacts in obtaining information according to federal and state law and third-party contractual obligations, Justifacts may perform periodic audits or be required to supply verification that Client is in compliance with this Agreement. Except for those documents hosted on Justifacts system, Client agrees to maintain in its records a copy of all consent forms, disclosures and pre-adverse and adverse action notices for a minimum of 5 years and Client shall, upon reasonable notice, provide Justifacts or its designated representatives such documents to show compliance with its obligations in this Agreement.

**2.7 Account Access.** Client shall designate a primary contact (Contact) for the Justifacts account who shall be responsible for the administration and control of Client's account. The Contact shall identify and authorize all Client users and their level of access to the Justifacts system and will promptly notify Justifacts of any changes to users or access privileges.

- 3. FEES.** Client agrees to pay Justifacts for providing Verification Services according to the Fee Schedule set forth in Exhibit "C". If Client requests additional services not initially set forth in the Fee Schedule, such added services will be hereby incorporated into this Agreement at Justifacts then-current rate unless otherwise mutually agreed-upon in writing by the parties. Client acknowledges that it will be responsible for charges resulting from its data input errors, duplicate requests and request cancellations initiated after processing has commenced. Client shall pay all pass-through fees incurred from information sources (including but not limited to The Work#, National Student Clearinghouse, DMV, courts, etc) for release of information or records used in compiling the Verification Services. Such pass-through fees are subject to change without prior notice. If at any time there are any changes in laws or government regulations that increase Justifacts cost to provide services or reasonably requires additional services to be provided by Justifacts, or in Justifacts determination restrict its ability to reasonably continue to provide the service(s) in this Agreement, Justifacts may, upon providing prior written notice to Client: (i) add a reasonable fee or pricing change to cover the added costs of providing the affected service(s), and/or (ii) modify or cease providing the affected service(s). Justifacts will

conduct annual audits of Client account to determine order history, number of reports requested and criminal hit ratio (Number of reports with a criminal record/total number of criminal record reports requested). If the volume of requests does not meet anticipated levels, Justifacts may, upon providing 30-day prior written notice to Client, increase the cost of services provided to meet the actual volume of report requests. If the hit ratio for criminal records exceeds 25%, Justifacts may, upon providing 30-day prior written notice to Client, increase the cost of criminal record search requests to meet the higher rate of criminal records found.

4. **PAYMENTS.** Justifacts shall invoice Client on a monthly basis and Client will promptly review each invoice and notify Justifacts of any errors or disputes on or before the due date of such invoice. Within thirty (30) days of the date of an invoice from Justifacts, Client will submit payment for all undisputed amounts. If all undisputed amounts are not received by Justifacts by the due date, Justifacts may: (i) suspend Client's account until all delinquent payments are received, and/or (ii) charge Client a finance charge of 1½% per month or a minimum of \$1, whichever is greater, and/or (iii) charge a late fee of \$15 for all undisputed amounts outstanding over 60 days. In the event of a dispute regarding fees or charges, the parties will use reasonable efforts to discuss in good faith and come to an agreement regarding resolution of such dispute. All amounts to be paid herein will be in U.S. Dollars.

## 5. **TERM AND TERMINATION.**

**5.1 Term.** The term of this Agreement will be one (1) year from the date of this Agreement unless otherwise terminated as provided herein. The term of this Agreement shall automatically renew on a month-to-month basis until either party terminates the agreement by giving the other party not less than thirty (30) days written notice of termination before the end of the then current term.

**5.2 Material Breach.** For the purposes of this Agreement, Justifacts will be deemed to be in material breach of this agreement in that event that; (i) there are consistent or repeated material errors or inaccuracies with regard to the Verification Services provided by Justifacts of which Justifacts has prior notice from Client, and for which an opportunity to cure was provided; or (ii) Client receives repeated complaints from Client Representatives regarding the Verification Services, Justifacts has notice of such complaints and such complaints are not resolved to the satisfaction of Client. For the purposes of this agreement, Client will be in material breach of this agreement in the event that (i) its determined that Client is not in compliance with any federal or state law concerning the request, use or dissemination of information contained in the consumer reports provided by Justifacts, (ii) information is being requested by Client users on themselves or on individuals who have not properly authorized the collection or use of the information (iii) information is being resold or (iv) Client fails to pay invoice within the agreed payment terms. If either party is deemed to be in material breach, the non-breaching party may terminate this Agreement immediately upon written notice that the material breach remains uncured fifteen (15) days after the breaching party's receipt of the written notice of the breach pursuant to Section 5.3 (i) below.



**5.3 Termination.** This Agreement may be terminated by the parties as follows: (i) Either party may terminate this Agreement at any time in the event of a material breach by the other party of any provision of this Agreement that remains uncured fifteen (15) days after the breaching party's receipt of written notice of the breach; (ii) Either party may terminate this Agreement immediately if the other party becomes insolvent, or is unable to pay its debts or perform its obligations when due, or enters into or files (or has filed or commenced against it) a petition, arrangement, action or other proceeding seeking relief or protection under the bankruptcy laws of the United States or similar laws of the United States or any state of the United States or transfers all of its assets to another person or entity.

6. **WARRANTY.** Each party warrants and represents to the other party that it has full power and authority to enter into this Agreement and to carry out its obligations hereunder. Justifacts warrants to Client that (i) Justifacts has the authority to perform the Verification Services; (ii) during the term of this Agreement, Justifacts will comply with all laws applicable to the performance of the Verification Services as well as preparation, content, licensing, distribution and transmission of the products or services offered for sale on the Justifacts website in each jurisdiction where such compliance by Justifacts is necessary. Client warrants to Justifacts during the term of this Agreement, Client will comply with all laws applicable to the Client in respect to the preparation, content, licensing, distribution and transmission and use of the Verification Services provided by Justifacts.
  
7. **INDEMNITY.** Client agrees to defend, indemnify and hold Justifacts harmless from any and all liabilities, damages, claims, and cost of defense or actions arising out of any claim (a) relating to the performance or breach of Client's obligations or responsibilities under this Agreement; (b) relating to the preparation, submission, dissemination or any information contained in a report under dispute by a consumer, provided that Justifacts promptly notifies Client of the consumer dispute and Client takes any adverse action against the consumer prior to receiving notification of the resolution of same from Justifacts. This indemnification and hold harmless provision will extend to damages, costs, and the expense of defending any claim against Justifacts. Justifacts will promptly notify Client of any suit or threat of suit that may obligate Client to indemnify Justifacts under the above provisions and be given reasonable opportunity to defend same. Justifacts will reasonably cooperate with Client with regard to the defense of any suit or threatened suit and Client will have authority to settle, pay or otherwise dispose of any such suit or threatened suit, subject to the approval of Justifacts, which approval will not be unreasonably withheld.

Justifacts agrees to defend, indemnify and hold Client harmless from any and all liabilities, damages, claims, and cost of defense or actions arising out of any claim (a) relating to the performance or breach of Justifacts obligations or responsibilities under this Agreement. This indemnification and hold harmless provision will extend to damages, costs, and the expense of defending any claim against Client. Client will promptly notify Justifacts of any suit or threat of suit that may obligate Justifacts to indemnify Client under the above provisions and be given reasonable opportunity to defend same. Client will reasonably cooperate with Justifacts with regard to the defense of any suit or threatened suit and Justifacts will have authority to settle, pay or otherwise dispose of any such suit or threatened suit, subject to the approval of Client, which approval will not be unreasonably withheld.

8. **WARRANTY DISCLAIMER.** EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER PARTY MAKES, AND EACH PARTY SPECIFICALLY DISCLAIMS, ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE, AND IMPLIED WARRANTIES ARISING FROM COURSE OF DEALING OR PERFORMANCE.

9. **LIMITATION OF LIABILITY.** EXCEPT WITH RESPECT TO (I) EACH PARTY'S INDEMNITY OBLIGATIONS HEREUNDER, (II) BREACHES OF CONFIDENTIALITY OBLIGATIONS UNDER SECTION 10, AND (III) ACTS OF GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND WHETHER OR NOT SUCH DAMAGES WERE FORESEEABLE, AND WHETHER OR NOT THAT PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## 10. CONFIDENTIALITY.

**10.1 Confidential Information.** "Confidential Information" will mean and refer to information about the disclosing party's (or its suppliers) business or activities that is proprietary and confidential including but not limited to: (i) any and all information relating to the consumer reports created at the request of Client; (ii) any and all information contained in any usage reports or related to all terms and conditions of this Agreement and all attachments hereto; (iii) all business, financial, technical and other information of a party marked or designated by such party as "*confidential*" or "*proprietary*"; or (iv) information which, by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as confidential.

**10.2 Exclusions.** Confidential Information will not include information that (i) is in or enters the public domain without breach of this Agreement, (ii) the receiving party lawfully receives from a third party without restriction on disclosure and without breach of a nondisclosure obligation or (iii) the receiving party knew prior to receiving such information from the disclosing party or (iv) the receiving party develops independently of the other party's Confidential Information.

**10.3 Use and Disclosure Restrictions.** Each party agrees (i) that it will not disclose to any third-party or use any Confidential Information disclosed to it by the other except as expressly permitted in this Agreement and (ii) that it will take all reasonable measures to maintain the confidentiality of all Confidential Information of the other party in its possession or control, which will in no event be less than a reasonable degree of care. Notwithstanding the foregoing, each party may disclose Confidential Information (i) to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required by law or (ii) on a "need-to-know" basis under an obligation of

confidentiality to its legal counsel, accountants, banks and other financing sources and their advisors or (jii) to the extent needed to complete the requested Verification Services.

## 11. GENERAL.

**11.1 Modification.** Any amendment, modification, supplement, or other change to any provision of this Agreement must be in writing and signed by both parties. All amendments or modifications of this Agreement will be binding upon the parties despite any lack of consideration so long as such amendments or modifications are in writing and executed by the parties.

**11.2 Waiver.** All waivers must be in a writing signed by the waiving party. The failure of either party to insist upon strict performance of any provision of this Agreement, or to exercise any right provided in this Agreement, will not be considered a waiver for the future exercise of such provision or right. No waiver of any provision or right will affect the right of the waiving party to enforce any other provision or right in this Agreement.

**11.3 Independent Parties.** The parties to this Agreement are independent parties and nothing herein will be construed as creating an employment, agency, joint venture or partnership relationship between the parties. Neither party will have any right, power or authority to enter into any agreement for or on behalf of, or incur any obligation or liability, or to otherwise bind, the other party.

**11.4 No Assignment.** Neither party may assign their obligations or rights under this Agreement without the other party's written consent, provided that either party may assign this Agreement without the other's consent to a successor in interest in the event of a reorganization, merger, consolidation, or sale of all or substantially all of its assets.

**11.5 Compliance with Laws.** Each party will comply with all laws, rules, and regulations of the United States. This Agreement is in the English language only, which language will be controlling in all respects, and all versions of this Agreement in any other language will be for accommodation only and will not be binding upon the parties hereto. All communications and notices to be made or given pursuant to this Agreement will be in the English language.

**11.6 Jurisdiction.** The Agreement will be governed by the internal laws of the state of Pennsylvania without regard to conflict of laws provisions. Client hereby irrevocably consents to the personal jurisdiction of the federal and state courts sitting in Allegheny County in the State of Pennsylvania, and to service of process within or without Pennsylvania. Client further agrees that any court action relating to the enforcement of any judgment or seeking injunctive or other equitable relief will be brought in such courts.

**11.7 Construction.** Except as specifically provided in this Agreement, all notices required hereunder will be in writing and will be effective when received. This Agreement, including any exhibits attached hereto, constitutes the entire understanding and agreement with respect to its subject matter, and supersedes any and all prior or contemporaneous representations, understandings and agreements whether oral or written between the parties relating to the subject matter of this Agreement. In the event that any provision of this Agreement is found to be invalid or unenforceable pursuant to judicial decree or decision,

the remainder of this Agreement will remain valid and enforceable according to its terms. The section and paragraph headings used in this Agreement are inserted for convenience only and will not affect the meaning or interpretation of this Agreement.

The parties have duly executed this Agreement by the authorized signatures below.

Client:	<u>CITY OF GRAND JUNCTION</u>	Justifacts Credential Verification, Inc.
By:	<u><i>Claudia Hazelhurst</i></u>	By: <u><i>Andrew Yober</i></u>
Name:	<u>CLAUDIA HAZELHURST</u>	Name: <u>Andrew Yober</u>
Title:	<u>HUMAN RESOURCES DIRECTOR</u>	Title: <u>VP - Criminal Records</u>
E-Mail:	<u>CLAUDIAH@GJ.CITY.ORG</u>	Date: <u>06/21/18</u>
Date:	<u>JUNE 4, 2018</u>	

## Exhibit A - AGREEMENT TO ABIDE BY THE FAIR CREDIT REPORTING ACT

Client certifies and agrees:

That it will comply with the Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (hereinafter FCRA) and all other applicable statutes, both state and federal.

That each request for a consumer report or an investigative consumer report is being obtained for the following purposes and for no other purpose:

- (A) for employment purposes
- (B) in connection with a business transaction involving the consumer, which is:
- \_\_\_\_\_
- (C) In accordance with the written instructions of the consumer

That information will be requested only for the Client's exclusive use and will not be otherwise distributed or sold. Client shall use each Consumer Report only for one time use and shall hold the report in strict confidence, except to the extent permitted by law. Reports on employees will be requested only by Client's designated representatives. Client users are forbidden to attempt to obtain reports on themselves, associates, or any other person except in the exercise of their official duties.

That each time a request for a consumer report and/or a investigative consumer report is made of Justifacts for employment purposes, Client will comply with §604(b) and §606(a) of the FCRA and that each time a request for an investigative consumer report is made of Justifacts for any non-employment purpose, Client will comply with §606(a) of the FCRA:

§604(b): (1) the consumer has been given a clear and conspicuous written disclosure, in advance (in a document that consists solely of the disclosure), that a consumer report may be requested for employment purposes; (2) the consumer has authorized the Client, in writing, to procure the report; (3) the information in the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation as well as any law providing consumer credit or consumer identity protection; (4) before taking adverse action, based in whole or in part on the report, Client will; (a) provide the consumer a copy of the report and a copy of "The Summary of Your Rights under the FCRA"; (b) allow the consumer a designated period of time to contact Justifacts if the consumer wishes to dispute any information in the consumer report; (c) provide the Justifacts contact information; and (d) provide a final adverse action notice to the consumer if a final adverse employment decision is made.

§606(a): (1) provide the consumer with a clear and accurate written disclosure, no later than three days after the report is requested, that a report may be made including information as to their character, general reputation, personal characteristics and mode of living; (2) provide the consumer a copy of the "Summary of Your Rights under the FCRA"; (3) provide a statement that the consumer has the right to request additional disclosures and to provide these disclosures when requested by the consumer.

That Client has received the following notices prescribed by the FCRA: (1) Notice to Users of Consumer Reports; (2) A Summary of Your Rights under the FCRA; and (3) Remedying the Effects of Identity Theft. It is incumbent upon the client to engage its own legal counsel to ensure that they are in compliance with all requirements of the FCRA as well as all state and federal employment law.

The individual whose signature appears below represents that they are authorized to enter into this agreement on behalf of the Client.

**CLIENT**

Company: CITY OF GRAND JUNCTION

Signature: *Claudia Hazelhurst*

Print Name: CLAUDIA HAZELHURST

Title: HUMAN RESOURCES DIRECTOR

Date: JUNE 4, 2018

**ACCEPTED BY**

Justifacts Credential Verification, Inc.

Signature: *Andrew Yoder*

Print Name: Andrew Yoder

Title: VP - Credential Records

Date: 06/21/18

## Exhibit B - Access Security Requirements

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is Clients responsibility to implement these controls. Justifacts reserves the right to make changes to the Access Security Requirements without notification.

Client understands that the access security requirements are comprehensive and that some requirements may not apply if reports are being stored on Justifacts system only and not electronically stored by me. In accessing the services provided by Justifacts, Client agrees to follow these security requirements:

### 1. Implement Strong Access Control Measures

- 1.1 Do not provide your account Access Codes or passwords to anyone. No one from Justifacts will ever contact you and request your Access Codes or password.
- 1.2 Proprietary or third party system access software must have Access Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Access Code / password be changed immediately when:
  - Any system access software is replaced by system access software or is no longer used;
  - The hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect Justifacts Access Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Access Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
  - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to Justifacts information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to Justifacts information.
- 1.12 Ensure that personnel who are authorized access to Justifacts information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your client application.
- 1.13 Ensure that you and your employees do not access your own background/credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a business transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access Justifacts information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- 1.15 After normal business hours, turn off and lock all devices or systems used to access Justifacts reporting systems and information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain background reporting and credit information.

## 2. Maintain a Vulnerability Management Program

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 2.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best 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.
- 2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
  - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
  - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
  - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
  - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
  - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
  - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
  - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company'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.

## 3. Protect Data

- 3.1 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.)
- 3.2 All Justifacts background reporting and credit data is classified as Confidential and must be secured to this requirement at a minimum.
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all Justifacts reports and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

## 4. Maintain an Information Security Policy

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.



## 5. Build and Maintain a Secure Network

- 5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 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.
- 5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

## 6. Regularly Monitor and Test Networks

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access Justifacts systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
  - protecting against intrusions;
  - securing the computer systems and network devices;
  - and protecting against intrusions of operating systems or software.

## Exhibit C – Fee Schedule

Justifacts Credential Verification, Inc Background Check solution includes:

### Background Check Package (Colorado)

Statewide Unified Criminal Court Search*	\$14.00	per name
National Criminal Database Search** (Includes Sex Offender Registry)	\$6.00	per name
Federal District Criminal Court Search	\$6.00	per name
Social Security Trace (Name & Address Verification)	\$2.00	

Base Total: **\$28.00**

### Background Check Package w/ MVR (Colorado)

Statewide Unified Criminal Court Search*	\$14.00	per name
National Criminal Database Search** (Includes Sex Offender Registry)	\$6.00	per name
Federal District Criminal Court Search	\$6.00	per name
Social Security Trace (Name & Address Verification)	\$2.00	
Motor Vehicle Record Check*	\$5.00	per check

Base Total: **\$33.00**

### Background Check Package (Out-of-State)

Best Practices Criminal Court Search*	\$19.95	per name
National Criminal Database Search** (Includes Sex Offender Registry)	\$6.00	per name
Federal District Criminal Court Search	\$6.00	per name
Social Security Trace (Name & Address Verification)	\$2.00	

Base Total: **\$33.95**

### Background Check Package w/ MVR (Out-of-State)

Best Practices Criminal Court Search*	\$19.95	per name
National Criminal Database Search** (Includes Sex Offender Registry)	\$6.00	per name
Federal District Criminal Court Search	\$6.00	per name
Social Security Trace (Name & Address Verification)	\$2.00	
Motor Vehicle Record Check*	\$5.00	per check

Base Total: **\$38.95**

**Individual Options** *Add any of the below searches to a package or order individually*

1	Single County Criminal Court Search*	\$11.00	per name
2	State Criminal Record Check*	\$6.00	per name
3	National Criminal Database Search**	\$6.00	per name
4	Federal District Criminal Court Search	\$6.00	per name
5	Motor Vehicle Record Check*	\$5.00	per record
6	Confirmation of Degree/Education*	\$8.00	per degree
7	Professional License Verification	\$8.00	per license
8	Basic Employment Verification*	\$9.50	per employer
9	Comp Plus Employment Verification*	\$14.00	per employer
10	Credit Check (Experian)	\$6.50	per report
11	5 or 10 Panel Drug Test-Urinalysis***	\$30.00	per test

Service	Price
Account set-up and access levels for unlimited Client users	Included
Online report ordering and retrieval	Included
Online Applicant web portal	Included
Online Administrative Reports	Included
Online Adverse Action Letters	Included
Online Resource Center	Included
ATS/HRIS integration	Included
U.S. Based Customer Support (Telephone, email, live chat)	Included
Automated status notifications	Included
Individualized Assessment Tool	Included

Optional Features:

- Applicant Tracking System
- Electronic I9 System
- Employee Monitoring System
- Adverse Action Letter Handling
- CA applicant check box/AB 1068 report delivery
- Order Entry
- System Customization options

Fees levied by Federal, State, County and other governmental agencies for searches undertaken will be passed through to Subscriber in addition to the fees charged by Justifacts. Such fees may include case copies associated with records found, administrative fees, and/or third-party fees. Additional criminal searches including counties added by Subscriber outside of those found by the social trace, including aliases and maiden names will be billed at a la carte rates.

Fees levied by educational institutions and/or employers and those who have retained third party vendors to respond to requests for verifications of education and employment will be passed through to Subscriber in addition to the fees charged by Justifacts.

National Criminal Database: if a criminal record is indicated on the National Criminal Database search, the appropriate county criminal record search will automatically be added at the additional county search cost.

Drug/Medical Testing Pricing:

In Network : All drug/medical testing performed at In Network collection facilities (LabCorp or Quest owned Patient Service Centers or other laboratory-owned and managed collection facilities authorized for Subscriber's use, but excluding laboratory preferred third party network collection sites) includes the cost of specimen collection, laboratory testing and MRO review.

Preferred Third Party Network Fee: The "Preferred Network" drug/medical testing service fee is incurred when using a Preferred Clinic Network facility.

Out of Network Fee: The "Out of Network" drug/medical testing service fee is incurred when using collection facilities that are Out of Network (i.e., not pre-established and authorized for Subscriber's program).

Additionally, there is a \$0.25 security/compliance fee per each report requested.

# Client Application



Justifacts Credential Verification, Inc.  
5250 Logan Ferry Road  
Murrysville, PA 15668  
PH (412) 798-4790 FX (412) 798-4799

Date of Application: 06/04/2018

Important: All information must be completed in its entirety. Please print clearly and legibly to ensure accurate and timely processing.

## General Company Information

Company Name: CITY OF GRAND JUNCTION Years in Business: \_\_\_\_\_ Yrs \_\_\_\_\_ Mo

Type of Ownership (indicate one):  Partnership  Sole Owner  Nonprofit  Corporation  LLC  LLP

LOCAL GOVERNMENT (LOCAL)  
Do you have any other company name(s) or dba?  Yes  No If Yes, please list: \_\_\_\_\_

Please describe the nature of your business: Local Government

FEIN Number: 84-6000592 State of Incorporation: Colorado

Physical Street Address (no. P.O. box numbers, please): 250 N. 5th Street

City: Grand Junction State: CO ZIP: 81501 How Long: \_\_\_\_\_ Yrs \_\_\_\_\_ Mo

Corporate Phone: (970) 244-1515 Fax: ( ) Is this a residential address?  Yes  No

Previous Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ ZIP: \_\_\_\_\_ How Long: \_\_\_\_\_ Yrs \_\_\_\_\_ Mo

Do you own or lease the building in which you are located? (please check one):  Own  Lease

## Primary Contact

Contact Name: Capri George

Title or Position: Senior HR Assistant

Phone: (970) 256-4140

Supervisor Name: Shelley Caskey

Supervisor Title: HR Supervisor

Address: 250 N. 5th Street

City: Grand Junction

State: CO

Zip: 81501

## Affiliated or Parent Company Information

Affiliated or Parent Company Name: \_\_\_\_\_

Contact Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: ( ) \_\_\_\_\_

City: \_\_\_\_\_

State: \_\_\_\_\_

Zip: \_\_\_\_\_

**Justifacts Credential Verification  
Membership Application – Continued**

<b>Permissible Purpose/Appropriate Use</b>	(Application will not be processed unless this information is provided.)
Please describe the <u>specific</u> purpose for which Justifacts product information will be used. (What will you do with the information obtained?)	
This section <b>MUST</b> be completed. Provide additional Detail if Necessary	
<input checked="" type="checkbox"/> Employment Background Screening <input type="checkbox"/> Tenant Background Screening <input type="checkbox"/> Other – Provide Detailed Description of Purpose	

I certify that my business is not included on the list of "Unauthorized End Use Business Types". I have read and understand the "Notice to Users of Consumer Reports" and the "Access Security Requirements" and will take all reasonable measures to enforce them within my facility. I understand that the access security requirements are comprehensive and that some requirements may not apply if reports are being stored on Justifacts system only and not electronically stored by me. I certify that I am the end user of all information provided by Justifacts Credential Verification and will use this information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. I will not resell the report to any third party. I understand that if Justifacts' system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated.

CITY OF GRAND JUNCTION  
Company Name

CLAUDIA HAZELHURST  
Type or Print Name of Authorized Person

*[Handwritten Signature]*  
Authorized Signature

HUMAN RESOURCES DIRECTOR  
Title

JUNE 4, 2018  
Date