Justifacts Client Startup Package

Justifacts
Credential Verification, Inc.

Justifacts Credential Verification, Inc.

Last Revised on **02/18/2021**

Attached you will find documents and information that you will need to get started with Justifacts. These include:

Credential Verification Service Agreement – This agreement needs to be completed and executed prior to initiation of services to client.

Exhibit A - Agreement to Abide By The Fair Credit Reporting Act (FCRA)

Exhibit B –Access Security Requirements

Exhibit C – Fee Schedule

Client Application

New Client Profile – The information you provide on the New Client Profile helps your dedicated account manager and his/her team to understand your company and your background screening preferences.

Information for your files – This information includes standard requirements under the FCRA. *Please carefully review the Notice to Users of Consumer Reports*. If you have questions regarding your obligations under the FCRA, please contact your Sales Manager.

Please complete and return the Credential Verification Service Agreement and exhibits, Client Application and New Client Profile

Remainder is for your records – please save/store for future reference

Please feel free to call with any questions!
800-356-6885

Mike Jackson – Sales Representative
Justifacts Credential Verification, Inc.

Justifacts Credential Verification, Inc
Credential Verification Service Agreement

This Credential Verification Service Agreement ("Agreement") is entered into and effective as of March 2, 2021 ("Effective Date"), by and between **Justifacts Credential Verification, Inc.** ("Justifacts"), a Pennsylvania Corporation with offices at 5250 Logan Ferry Road, Murrysville PA 15668 and The City of El Mirage ("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. **OBILIGATIONS 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 initiated 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 Justiweb 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 or shared with third parties. 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; and (2) Summary of Consumer rights under the FCRA.

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, Justifacts recommends 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. Accepted forms of payment are check, ACH, and credit card ; funds remitted via credit card will be subject to a 3% fee on the gross invoice amount. 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 three (3) years 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 users 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 Clients 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.

10.4 Personal Data Breach Each Party shall promptly notify the other Party upon becoming aware of a Personal Data Breach affecting Confidential Information. Such notification shall, as a minimum, include sufficient information to allow either Party to fulfill its obligations under applicable law, including: (i) description of the nature of the breach; (ii) the Confidential Information involved; and (iii) description of the measures taken or proposed to be taken to address the breach.

Each Party shall cooperate with the other Party and take reasonable commercial steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

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: _____

By: _____

Name: _____

Title: _____

E-Mail: _____

Date: _____

Justifacts Credential Verification, Inc.

By: _____

Name: Andrew Yoder

Title: VP- Criminal Records

Date: 05/18/21

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:

_X_ (A) for employment purposes

___ (B) in connection with a business transaction initiated by the consumer, which is:

_____

___ (C) In accordance with the written instructions of the consumer

That information will be requested only for the Clients 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 has complied with §604(b)(1) and §604(b)(2) and will comply with §604(b)(3), §604(b)(4) and §606(a) of the FCRA and that each time a request for an investigative consumer report is made of Justifacts for any **any 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; and (2) Summary of Consumer rights under the FCRA. 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: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

ACCEPTED BY

Justifacts Credential Verification, Inc.

Signature: _____

Print Name: Andrew Yoder

Title: VP - Collateral Records

Date: 05/18/21

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.

Justifacts 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, Justifacts recommends that Client 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:

Service	Price

All Areas of Residence Per Name for 7 Years Package:

• Social Security Trace *(Name and address history)*	$ 1.95
• All Counties of Residence Criminal Record Search* *(Searches all areas of Residence in the past 7 years as per the Social Security Trace, per name)*	$18.00
• National Criminal Database (*Multistate criminal record search, includes 50 state sex offender registry, GSA, OIG and OFAC government watch list)(per name)*	$5.00
• Comprehensive Employment Verification* *(Verifies up to 3 employers within the last 7 years. Job title, employment dates, salary, reason for leaving, and rehire eligibility will be verified. This also includes a minimum 2 performance reviews from supervisors, or references will be substituted)*	$30.00
• Federal District Criminal Record Check*	$5.00
• Confirmation of Degree*	$6.00
• Motor Vehicle Record Check*	$3.00

Total: $68.95

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

DOT Employment Verifications (Per Verification).....$10.00

Additional Employment or Reference Checks (each).....$15.00

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).

Reschedule Fee: There is a $5 reschedule fee for any drug/\medical test that needs to be rescheduled due to expiration of the original request or to obtain a different collection location.

Certificate Fee: There is a $1 fee to have drug test certificates uploaded to the Justifacts system when using services that do not automatically include the certificate upload.

Public Record Fees:

1) State/County/Unified Court fees– Some jurisdictions impose fees to access their information. All governmental fees to access records are passed through to client.
2) Case copies – In those instances where case copies are required, Justifacts passes through any associated costs with obtaining copies of court cases.
3) Archive fees – In those instances where a case is archived, some jurisdictions charge fees to retrieve archived cases. Justifacts passes through all costs associated with obtaining archived files.
4) Out of Scope fees – in those instances where a client requires a case outside of the normal 7-year scope of a Justifacts report, additional fees may be imposed.
5) Excessive case fees – Justifacts will charge fees on a per-case basis when a requested search returns more than 15 cases on an individual. This fee varies based on jurisdiction.
6) Civil Record Fees – All civil searches are searches of the courts name index only. Any case found must be ordered at additional cost to confirm personal identifiers

There is a one-time $65 start-up fee and a $.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:

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: _____ Years in Business: _____ Yrs _____ Mo

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

Do you have any other company name(s) or dba? ☐ Yes ☐ No If Yes, please list: _____

Please describe the nature of your business:

FEIN Number: State of Incorporation:

Physical Street Address (no. P.O. box numbers, please): _____

City: _____ State: _____ ZIP: _____ How Long: _____ Yrs _____ Mo

Corporate Phone: (623) 972-8116 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: _____

Title or Position: _____ Phone: ( )

Supervisor Name: _____ Supervisor Title: _____

Address: _____

City: State: Zip:

Affiliated or Parent Company Information

Affiliated or Parent Company Name: _____

Contact Name: _____ Title: _____

Address: _____ Phone: ( )

City: State: Zip:

Justifacts Credential Verification Membership Application – Continued

Permissible Purpose/Appropriate Use	(Application will not be processed unless this information is provided.)
Please describe the **specific** purpose for which Justifacts product information will be used. (What will you do with the information obtained?)	
This section MUST be completed. Provide additional Detail if Necessary	
☒ Employment Background Screening	
☐ Tenant Background Screening	
☐ 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.

Company Name

Type or Print Name of Authorized Person

Title

Authorized Signature

Date

Please complete the New Client Profile. As a client of Justifacts, your organization will have an Account Manager that is assigned to process your requests. He or she has a team of research specialists that will handle each facet of your order. The New Client Profile will help the Account Manager process your requests based on your preferences. Once we receive your first job, we will provide you with the name and contact information for your Account Manager.

1. How did you hear about Justifacts?

2. How many employees and or contractors are employed by your company?

3. Approximately how many applicants / existing employees do you anticipate ordering background reports for each month?

4. Does your company extend a job offer to the applicant prior to conducting the background search?
☐ Yes ☐ No

5. When do you anticipate sending in your first job?

6. Will you provide us with the applicant's Date of Birth information as requested on the applicant release?
☐ Yes ☐ No **(please note: With your permission Justifacts will contact the applicant to obtain the date of birth for you. That information will be kept confidential at Justifacts)**

7. Will Justifacts have permission to call the applicant when we need information that may be lacking in their application or resume? ☐ Yes ☐ No

8. Most of Justifacts background search packages include one county and/or state criminal record search. If additional addresses are located on an address information search or indicated by the applicant, would you like your account manager to automatically search criminal records for all addresses lived in the last 7 years at an additional charge? ☐ Yes ☐ No

9. Would you like Justifacts to conduct a criminal record search for all names and/or alias' used at an additional charge? ☐ Yes ☐ No

***Note: Justifacts recommends that you conduct criminal record searches for all names to assure an accurate search.**

10. Do you want an email confirming our receipt of your request? ☐ Yes ☐ No

11. In which State or States will the employees you hire be working? (Please note that State laws governing hiring practices differ in each state. This information will be used to determine which state will impact the information we report.)

12. Do you want an email confirming our receipt of your request and upon completion of the report?
☐ Yes ☐ No

13. Do you want Justifacts to notify you when a search you request requires us to use an automated system which results in an additional fee? ☐ Yes ☐ No

14. How do you prefer to submit your jobs to Justifacts?
☐ Justiweb (online) ☐ Electronic Candidate Portal ☐ File Upload System ☐ Fax

15. Please indicate the name of any specialized HR software used in your hiring process.

16. Beside yourself, will there be any other authorized users of the system? Also, is tiered access needed? If so, please provide the following information, job titles and what capacity they interact. (*Administrative*: can see/retrieve all reports entered by all users. *Regional*: can see/retrieve their own reports and Divisional user reports. *Divisional*: can only see/retrieve orders that they entered.) Please indicate if listed users are authorized to add new users to access the Justiweb system.

Name: **Title:**
Email Address:
Phone Number: **Fax Number:**

Access: ☐ Administrative ☐ Regional ☐ Divisional
Access to Credit Report Information (if requested) ☐ Yes ☐ No
Authorized to add new users ☐ Yes ☐ No

Name: **Title:**
Email Address:
Phone Number: **Fax Number:**

Access: ☐ Administrative ☐ Regional ☐ Divisional
Access to Credit Report Information (if requested) ☐ Yes ☐ No
Authorized to add new users ☐ Yes ☐ No

(Repeat as necessary)

17. To whom should Justifacts invoices be sent? Please include:
Name: **Title:**
Email Address:
Phone Number: **Fax Number:**
Mailing Address:

18. Do you prefer to receive the invoice via email or US Mail?

☐ Email ☐ Regular Mail

19. How does your company plan on paying invoices?
- ☐ **Check**
- ☐ **ACH**
- ☐ **Credit Card (Note: Credit Card payments subject to 3% service fee)**

20. Is your company interested in either a demonstration of or additional information regarding the applicant tracking system that Justifacts offers free of charge to our clients? ☐ Yes ☐ No

21. Is your company interested in either a demonstration of or additional information regarding the Electronic Form I-9 system that Justifacts offers to our clients? ☐ Yes ☐ No

23. How does your company plan on handling the adverse action process?
- ☐ **We plan on completing the process internally**
- ☐ **We plan on using Justiwebs' built in feature to complete the process**
- ☐ **We plan on having Justifacts complete the process using standard mail (At an additional charge)**
- ☐ **We plan on having Justifacts complete the process using certified mail (At an additional charge)**

24. For California, Minnesota and Oklahoma Applicants – Who is responsible for providing a copy of the background report to the applicant if the required Check Box on the Background Investigation Waiver is checked by the applicant requesting a copy of the report?

Client ☐ **Justifacts (At an additional fee)** ☐

Unauthorized End User Business Types

Justifacts periodically utilizes outside services to provide information requested as part of a background investigation. These services require that you provide a certification that you are not one of the following excluded entities. Businesses coming under any of the following categories may be excluded from receiving certain types of information.

Adoption Search Firms
Adult Entertainment service of any kind
Asset Location Services
Business operating out of a residence except where provided in policy
Bail Bond Enforcement or Bounty Hunter
Check cashing
Companies or Individuals identified on Experian Customer Alert List
Condominium/Homeowners Associations(unless acting as a tenant screener)
Country Clubs (Except for Employment screening)
Credit repair companies, Credit Clinics or For Profit Credit Counseling
Credit repair clinic or any type of company involved in credit repair activity
Dating service
Diet Centers
Financial counseling (except housing counseling agencies)
Future services (i.e., health clubs, continuity clubs, etc.), except health clubs (spas) human resource departments for employment screening
Genealogical or heir research firm
Internet People Locator Service
Investigative Companies, including Private Investigators and detective agencies except those licensed for – and exclusively practicing, investigative work for employment purpose
Law Enforcement (Except for Employment Screening)
Loan Modification Companies
Media agencies, News agencies or Journalists
Non-governmental agency or business associated with collection of child support
Pawn shop
Company that handles third party repossession
Company or individual involved in spiritual counseling
Subscriptions (magazines, book clubs, record clubs, etc.)
Timeshare (unless proof of credit extension is procured)
Any company or individual listed as a Specially Designated National on the Office of Foreign Asset Control (OFAC) website

As you may be aware, the information which you request and we provide is classified as a "consumer report" or "investigative consumer report" and is governed by the Fair Credit Reporting Act (FCRA). The FCRA provides protections and responsibilities to those who use information (our Clients), those upon whom the information is about (applicants or "consumers") and those who provide information (Justifacts). The full text of the FCRA, as amended, may be found on the Internet at: http://www.ftc.gov/sites/default/files/fcra.pdf

The following information provides details of your obligations under the FCRA. Please read the information carefully to ensure you understand the requirements that the FCRA places on you when you decide to include background information in your hiring process. Included are:

- Notice to users of consumer reports: Obligations of users under the FCRA
- Summary of Consumer rights under the FCRA

When requesting and using a background report, there are specific documents that must be presented to the subject of the report, depending on the purpose being requested. These include the following:

A. Consumer Report Disclosure
B. State Law Notices
C. Authorization to Conduct Background Investigation
D. Pre-Adverse Action Letter – Re: Employment
E. Adverse Action Letter

In addition to these documents, depending on the location of your facilities and applicants, there may be additional forms required. These include, but are not limited to:

- Notification and Authorization to Obtain Credit Report in California
- Notice to Obtain Credit Reports in Vermont

Justifacts can provide sample documents upon request. Contact your Sales manager for more information.

Due to the amount of regulation involving consumer reports (FCRA, EEOC, state law, etc), Justifacts strongly recommends that you consult with your legal counsel and other appropriate personnel to develop/review/implement a background screening policy and an adverse action process.

None of the information contained herein should be construed as legal advice, nor is Justifacts engaged to provide legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult your attorney or legal department if you require assurance that our information, and your interpretation of it, is appropriate to your particular situation. It is important that you work with your legal counsel to ensure that your policies and procedures related to the information received from Justifacts is in compliance with all applicable state and federal laws.

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's Website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Bureau's Web site. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a

telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the Consumer Financial Protection Bureau.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2)

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in regulations issued by the banking and credit union regulators) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, once the Consumer Financial Protection Bureau by rule has established the format, type size, and manner of the disclosure required by Section 615(d), users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  (1) the identity of all end-users;
  (2) certifications from all users of each purpose for which reports will be used; and
  (3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's Web site, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

Section 602	15 U.S.C. 1681
Section 603	15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681cA
Section 605B	15 U.S.C. 1681cB
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 612	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 1681l
Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 1681o
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 1681r
Section 621	15 U.S.C. 1681s
Section 622	15 U.S.C. 1681s-1
Section 623	15 U.S.C. 1681s-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y

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

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. **For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.**

- **You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.

- **You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

    - a person has taken adverse action against you because of information in your credit report;
    - you are the victim of identity theft and place a fraud alert in your file;
    - your file contains inaccurate information as a result of fraud;
    - you are on public assistance;
    - you are unemployed but expect to apply for employment within 60 days.

    In addition, all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.consumerfinance.gov/learnmore for additional information.

- **You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

- **You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.consumerfinance.gov/learnmore for an explanation of dispute procedures.

- **Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete, or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

- **Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

- **Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need – usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

- **You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.consumerfinance.gov/learnmore.

- **You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address form the lists these offers are based on. You may opt out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).

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

  CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

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

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

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

- **You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

- **Identity theft victims and active duty military personnel have additional rights.** For more information, visit www.consumerfinance.gov/learnmore.

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General. For information about your federal rights, contact: **TYPE OF BUSINESS:**	**CONTACT:**
1.a. Banks, savings associations, and credit unions with total assets of over $10 billion and their affiliates b. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the CFPB:	a. Consumer Financial Protection Bureau 1700 G Street, N.W. Washington, DC 20552 b. Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357
2. To the extent not included in item 1 above: a. National banks, federal savings associations, and federal branches and federal agencies of foreign banks b. State member banks, branches and agencies of foreign banks (other than federal branches, federal agencies, and Insured State Branches of Foreign Banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act. c. Nonmember Insured Banks, Insured State Branches of Foreign Banks, and insured state savings associations d. Federal Credit Unions	a. Office of the Comptroller of the Currency Customer Assistance Group 1301 McKinney Street, Suite 3450 Houston, TX 77010-9050 b. Federal Reserve Consumer Help Center P.O. Box 1200 Minneapolis, MN 55480 c. FDIC Consumer Response Center 1100 Walnut Street, Box #11 Kansas City, MO 64106 d. National Credit Union Administration Office of Consumer Financial Protection (OCFP) Division of Consumer Compliance Policy and Outreach 1775 Duke Street Alexandria, VA 22314
3. Air carriers	Asst. General Counsel for Aviation Enforcement & Proceedings Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, S.E. Washington, DC 20590
4. Creditors Subject to the Surface Transportation Board	Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, S.W. Washington, DC 20423
5. Creditors Subject to the Packers and Stockyards Act, 1921	Nearest Packers and Stockyards Administration area supervisor
6. Small Business Investment Companies	Associate Deputy Administrator for Capital Access United States Small Business Administration 409 Third Street, S.W., Suite 8200 Washington, DC 20416
7. Brokers and Dealers	Securities and Exchange Commission 100 F Street, N.E. Washington, DC 20549
8. Federal Land Banks, Federal Land Bank Associations, Federal Intermediate Credit Banks, and Production Credit Associations	Farm Credit Administration 1501 Farm Credit Drive McLean, VA 22102-5090
9. Retailers, Finance Companies, and All Other Creditors Not Listed Above	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357

Justifacts Credential Verification
5250 Logan Ferry Road
Murrysville, PA 15668
Email: customerservice@justifacts.com
Ph: (800) 356-6885
Fax: (412) 798-4799
www.Justifacts.com