Alliance2020
Insight is better than hindsight

Commercial Tenant Screening Reports

Master Service Agreement with Addendums

Commercial Tenant Screening Reports Welcome Packet

Welcome to Alliance 2020. Your membership packet includes several forms that you must complete before service can be started, as well as other items for your information.

You may fax the items listed below to Alliance 2020 at 800-289-9246. Scans of completed documents may be emailed to compliance@alliance2020.com.

Required Forms
The forms listed below must be completed, signed, dated and delivered to Alliance 2020, Inc.

- ☐ Application for Services Tenant Screening
- ☐ Master Agreement for Services Tenant Screening
- ☐ Credit Scoring Addendum
- ☐ Addendum: End Use Certification of Compliance California Civil Code – Section 1785.14(a)
- ☐ Addendum to Master Agreement for Services Certification that End User Will Comply with the Fair Credit Reporting Act
- ☐ FCRA Disclosure
- ☐ Death Master File Index Addendum

Business License
A copy of your business license must be delivered to Alliance 2020. This item is needed for Alliance 2020 to complete its due diligence.

- ☐ Copy of Your Current **Business License**

Required Site Inspection Will be Scheduled
Once we have received your forms, we will contact you to schedule a mandatory site inspection. Your packet includes information on this inspection and the items the inspector will be examining. You will not be given access to any credit reports until this inspection is completed.

Alliance 2020
Insight is better than hindsight

Application for Services Tenant Screening

Name of Firm or Individual (DBA, if applicable) Important: Must Match Business License	Telephone Number (including Area Code)		Fax Number
Physical Address	City	State	Zip code
Billing Address (if Different from Physical Address)	City	State	Zip code
Please Describe the Nature of the Business:		Date Established:	No. of Employees:

Intended use of Reports:	Estimated Number of Reports Per Month:	Reports are accessed: Locally ☐ Regionally ☐ Nationally ☐

This Business is a:

Corporation ☐ Partnership ☐ Sole Proprietorship ☐ LLC ☐ S-Corp ☐ Non Profit ☐ Other ☐

Website Address

BUSINESS LICENSE INFORMATION – A Copy of Business License Must Be Attached as Noted in New Account Checklist

Where is this business licensed? (County, City, State)	Business license number

ONE BUSINESS REFERENCE (Examples: Suppliers, Vendors, Contractors, etc.)

Company Name	Telephone Number	City	State	Zip code
Contact name:	Services purchased:			

AGREEMENT AND AUTHORIZATION

You understand and agree that you are limited to accessing Alliance 2020, Inc., information only for the permissible purpose of assessing individuals' background for employment-related purposes, in accordance with the Fair Credit Reporting Act(FCRA). Changes to your agreement must be made it writing and approved by Alliance 2020, Inc. prior to expanding/changing your access privileges.

By signing this form below, you authorize the release of all information requested by Alliance 2020, Inc. in the process of its due diligence. By signing this application, you indicate that you have the authority to enter into this agreement on behalf of yourself and/or the firm named above. You agree to pay for all services provided under this agreement. You acknowledge that you have read and accept, on behalf of yourself and/or the firm named above, the follow attached documents and certifications.

▶ _____ Authorized Individual Printed Name

▶ _____ Title

▶ _____ Authorized Individual Signature

▶ _____ Date

Master Service Agreement
Tenant Screening

This agreement, made on this date, _____, by and between Alliance 2020, Inc., a Washington Corporation with its principal place of business at 304 Main Ave South Suite 202, Renton, Washington, 98057, and _____, with its principal place of business at: _____, _____, _____, _____, (Subscriber/End User Address).

Subscriber/End User is a (describe your type of business) _____ and has a permissible purpose for obtaining consumer reports in accordance with the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) including, without limitation, all amendments thereto ("FCRA"). The End User certifies its permissible purpose as follows:

PROVISION OF CONSUMER INFORMATION

1. Subscriber certifies that consumer reports, as defined by the Federal Fair Credit Reporting Act, 15 U.S.C. Section 1681, seq. ("FCRA"), will be ordered only when intended to be used as a factor in establishing a consumer's eligibility for new or continued credit, collection of an account, insurance, licensing, tenant purposes, or otherwise in connection with a legitimate business transaction involving the consumer, and such reports will be used for no other purpose, including resale to the subject consumer or to another reseller or broker of consumer reports. Subscriber certifies that reports on its employees will be requested only by its designated representative. Subscriber employees will be forbidden to attempt to obtain reports on themselves or associates, or on any other person except in the exercise of their official duties. Subscriber further certifies that its policies and procedures are designed to comply with Section 1681(e) of the FCRA and other applicable state or federal laws.

   (A) End User certifies that End User shall use the consumer reports: (a) solely for the Subscriber's certified use(s); and (b) solely for End User's exclusive one- time use.
      i. End User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the consumer reports.
      ii. The consumer reports shall be requested by, and disclosed by End User only to End User's designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the Consumer Reports in accordance with this Agreement.
      iii. End User shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.

   (B) End User will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

   (C) THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18 OF THE UNITED STATES CODE OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.

   (D) END USER SHALL USE EACH CONSUMER REPORT ONLY FOR A ONE-TIME USE AND SHALL HOLD THE REPORT IN STRICT CONFIDENCE, AND NOT DISCLOSE IT TO ANY THIRD PARTIES; PROVIDED, HOWEVER, THAT END USER MAY, BUT IS NOT REQUIRED TO, DISCLOSE THE REPORT TO THE SUBJECT OF THE REPORT ONLY IN CONNECTION WITH AN ADVERSE ACTION BASED ON THE REPORT.
      I. MOREOVER, UNLESS OTHERWISE EXPLICITLY AUTHORIZED IN AN AGREEMENT BETWEEN RESELLER AND ITS END USER FOR SCORES OBTAINED FROM TRANSUNION, OR AS EXPLICITLY OTHERWISE AUTHORIZED IN ADVANCE AND IN WRITING BY TRANSUNION THROUGH RESELLER, END USER SHALL NOT DISCLOSE TO CONSUMERS OR ANY THIRD PARTY, ANY OR ALL SUCH SCORES PROVIDED UNDER SUCH AGREEMENT, UNLESS CLEARLY REQUIRED BY LAW.

(E) WITH JUST CAUSE, SUCH AS VIOLATION OF THE TERMS OF THE END USER'S CONTRACT OR A LEGAL REQUIREMENT, OR A MATERIAL CHANGE IN EXISTING LEGAL REQUIREMENTS THAT ADVERSELY AFFECTS THE END USER'S AGREEMENT, RESELLER MAY, UPON ITS ELECTION, DISCONTINUE SERVING THE END USER AND CANCEL THE AGREEMENT IMMEDIATELY.

(F) CLIENT ACKNOWLEDGES THAT IT IS FAMILIAR WITH AND AGREES TO COMPLY WITH THE REQUIREMENTS OF THE FAIR AND ACCURATE CREDIT TRANSACTION ACT (FACT ACT), THE GRAMM-LEACH-BLILEY ACT, (15 U.S.C.A., § 6801 ET. SEQ. (2000), ("GLB ACT") AND ALL REQUIREMENTS POSTED ON THE WEBSITE, IN CONNECTION WITH ORDERING, USING AND STORING CONSUMER AND/OR CREDIT REPORTS AND THE USE OF ANY CONSUMER DATA SUPPLIED BY OR ITS AFFILIATES. CLIENT ACKNOWLEDGES AND AGREES THAT IT IS SOLELY RESPONSIBLE FOR ITS OWN COMPLIANCE, ACCESS SECURITY AND ADHERENCE TO ALL APPLICABLE REGULATIONS.

(G) Subscriber has read and understands its obligations under the FCRA and the penalties for requesting consumer report information under false pretenses and signed a certification to this effect.

(H) Subscriber certifies it is not one of the businesses or business types listed on Exhibit A – Businesses Prohibited from Accessing Credit Reports Under this Agreement which is attached to this agreement. Nevertheless, Alliance 2020 may in its sole discretion deny access to Alliance 2020 information by certain applicants, even though otherwise "qualified." Subscriber releases Alliance2020, Equifax, Experian, TransUnion and its agents from any and all claims, demands, actions, causes for action, suits, costs, damages, expenses, compensation, penalties, liabilities and obligations of any kind or nature whatsoever arising out of or relating to such denial. Further, Subscriber/End-User covenants not to sue or maintain any claim, cause of action, demand, cross- action, counterclaim, third- party action or other form of pleading against Alliance 2020 arising out of or relating to such denial.

2. Subscriber understands that Alliance 2020 services will only be available to those applicants who have a FCRA permissible purposes listed in Section 1.

3. Subscriber will establish strict procedures so that subscriber employees or agents do not access Alliance 2020 Credit Information other than the permissible purpose. Alliance 2020 will immediately cease providing credit information to the subscriber that no longer has a permissible purpose under the FCRA.

4. Subscriber understands that Alliance 2020, Inc. may periodically audit subscriber requests regarding their compliance with the FCRA. Audits will be conducted by mail whenever possible and will require subscriber to provide documentation as to permissible uses of particular consumer reports. Subscriber will cooperate fully and promptly in the conduct of such audits.

5. If the disclosure of any information or reports by Subscribers leads to any claims or litigation, subscriber will indemnify Alliance 2020, Experian, TransUnion, Equifax, its agents, employees, and independent contractors, for any liability, damages or expenses resulting there from.

6. Subscriber shall refer all consumer disputes to Alliance 2020. Subscriber will establish strict procedures so that subscribers' employees and agents refer to Alliance 2020 all requests for disclosure from the subject to Alliance 2020.

7. Subscriber agrees to protect and dispose of consumer information in a manner agreeable to Alliance 2020.

8. Subscriber recognizes that the accuracy of any information furnished is not guaranteed by Alliance 2020, and releases Alliance 2020 and Alliance 2020s' agents, employees, credit reporting agencies (including but not limited to Equifax, Experian, TransUnion) and independent contractors from liability for any negligence in connection with the preparation of Alliance 2020 information, and from any loss or expense suffered by subscriber users resulting directly or indirectly from Alliance 2020 reports. Subscriber covenants not to sue or maintain any claim, cause of action, demand, cross-action, counterclaim, third-party action or other form of pleading against Alliance 2020, Alliance 2020s' agents, employees, credit reporting agencies (including but not limited to Equifax, Experian, TransUnion), and independent contractors arising out of or relating in any way to the accuracy or Inaccuracy, validity or no validity, or any of the Alliance 2020 credit information.

CREDIT SCORES

End User will request Scores only for End User's exclusive use. End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining the Scores. End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person, except (i) to those employees of End User with a need to know and in the course of their tenant; (ii) to those third party processing agents and other contractors of End User who have executed an agreement that limits the use of the Scores by the third party only to the use permitted to End User and contains the prohibitions set forth herein regarding model development, model calibration, reverse engineering and confidentiality; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; (iv) to government regulatory agencies; or (v) as required by law.

10. **DISCLAIMER OF WARRANTIES**
OTHER THAN THOSE EXPRESSED IN THIS AGREEMENT, ALLIANCE 2020, INC. MAKES NO REPRESENTATIONS, WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

11. If the disclosure of any information or reports by subscriber leads to any claims or litigation, subscriber will indemnify Alliance 2020, its agents, employees, affiliated credit reporting agencies (including but not limited to Equifax, Experian, TransUnion) and independent contractors for any liability, damage or expense resulting from that disclosure.

12. **EXHIBITS AND ADDENDUMS** All Exhibits and Addendums attached are a part of this Agreement and are expressly incorporated into it, and all blanks in the Exhibits and Addendums, if any, will be completed as required in order to consummate the transactions contemplated and in accordance with this Agreement

13. **WAIVER OF RIGHTS** Failure of any party to enforce any of its respective rights or remedies hereunder with respect to any specific act or failure to act of any party will not constitute a waiver of the rights of that party to enforce those rights and remedies with respect to any other or subsequent act or failure to act.

14. **CERTIFICATION STATEMENT** It is recognized and understood that the Fair Reporting Act provides that anyone who knowingly and willfully obtains information on a consumer from a consumer reporting agency (such as Alliance 2020, Inc. under false pretenses) may be liable to any consumer in an amount equal to the sum of:
    (A) Any actual damages sustained by the consumer as a result of the failure to comply.
    (B) Such amount of punitive damages as the court may allow
    (C) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court

15. **PAYMENT TERMS - ATTORNEY FEES** It is agreed all invoices are due and payable within twenty days of receipt. If payment is not received within twenty days, it is understood our account will be placed on hold until full payment is received. In the event our account is placed on hold, Alliance 2020, Inc., at its option, may require a deposit in the amount of our past two months billing. In the event our account is placed for collection, it is understood the prevailing party shall be entitled to reasonable attorney fees and collections fees. In any action or processing involving a dispute between the parties arising out of this agreement, the prevailing party shall be entitled to reasonable attorney fees.

16. **ENTIRE AGREEMENT**
This Agreement, including the Exhibits and Addendums hereto, constitutes the entire Agreement between the parties and supersedes and cancels any and all prior agreement between the parties relating to the subject matter. No changes in this Agreement may be made except in writing signed by both parties.

17. **TERM AND TERMINATION** This agreement remains in force but may be terminated by either party with or without notice. If the subscriber is delinquent in the payment of charges or is guilty of violating the term of this Agreement, Alliance 2020 may, at its election, discontinue providing services to Subscriber and cancel this Agreement immediately. In the event of termination of this Agreement for any reason, the provisions of the foregoing paragraphs will remain in full force and effect as to all Alliance 2020 which Subscriber has requested or received from Alliance 2020 prior to the cancellation date.

▶ _____ ▶ _____

AUTHORIZED INDIVIDUAL PRINTED NAME TITLE

▶ _____ ▶ _____

AUTHORIZED INDIVIDUAL SIGNATURE DATE

Accepted on Behalf of Alliance 2020:

▶ _____ ▶ _____ ▶ _____

AUTHORIZED INDIVIDUAL PRINTED NAME AUTHORIZED INDIVIDUAL SIGNATURE DATE

▶ _____ ▶ _____

TITLE EMAIL ADDRESS

Alliance2020
Insight is better than hindsight

Addendum to Master Service Agreement: Tenant Screening, Credit Scoring Services

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc., TransUnion LLC and Equifax Inc. (Credit Bureaus); and,

WHEREAS, Credit Bureaus and Fair, Isaac Corporation ("Fair, Isaac") offer three unique "Credit Bureaus/Fair, Isaac Models", (each Credit Bureau individually working with Fair, Isaac to develop their own unique model) consisting of the application of a risk model developed by each of the Credit Bureaus and Fair, Isaac which employs proprietary algorithms and which, when applied to credit information relating to individuals with whom the Subscriber/End-User contemplates entering into a credit relationship will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, for good and valuable consideration and intending to be legally bound, Subscriber/End-User and Provider hereby agrees as follows:

1. **General Provisions**
   - A. **Subject of Agreement.** The subject of this Agreement is Subscriber/End-User's purchase of Scores produced from the Credit Bureaus/Fair, Isaac Model from Provider.
   - B. **Application**. This agreement applies to all uses of the Credit Bureaus/Fair, Isaac Model by Subscriber/End-User during the term of this agreement.
   - C. **Term.** The term of this Agreement (the "Term") is the period consisting of the Initial Term and, if this Agreement is renewed, the Renewal Term(s), as follows:
     - i. Initial Term. The "Initial Terms" is the period beginning at 12:01 a.m. on the date written above and ending at 11:59 p.m. on the day before the first anniversary of that date in the time zone where Alliance 2020, Inc. Inc. is located.
     - ii. Renewal Term(s). Unless one of both of the parties delivers written notice of such party's (parties) intent not to renew no later than thirty (30) days before the end of the Initial Term, this Agreement will renew automatically and without further action by either party for an additional one-year period (a "Renewal Term"). Thereafter, this Agreement will continue to renew automatically unless and until either party delivers nonrenewable notice no later than thirty (30) days before the end of a Renewal Term. This Agreement will terminate without further action by either of the parties in the even Subscriber discontinues use of the Scoring Model.

2. **Credit Bureaus/Fair, Isaac Scores**
   - A. **Generally.** Upon request by Subscriber/End-User during the Term, Provider will provide Subscriber/End-User with the Scores in a timely manner.
   - B. **Warranty.** Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores will not contain or use any prohibited basis as defined by the Federal Equal Credit Opportunity Act, 15 USC Section 1691 *et seq.* or Regulation B promulgated hereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN SUBSCRIBER/END-USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN SUBSCRIBER/END-USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Subscriber/End-User's rights under the foregoing warranties are expressly conditioned upon Subscriber/End-User's periodic revalidation of the Credit Bureaus/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*).
   - C. **Release**. Subscriber/End-User hereby releases and holds harmless Provider, Fair Isaac and/or Credit Bureaus and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Credits Bureaus from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by Subscriber/End-User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

3. **Intellectual Property**
   A. **No License.** Nothing contained in this Agreement shall be deemed to grant Subscriber/End-User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Credit Bureaus and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. Subscriber/End-User acknowledges that the Credit Bureaus/Fair, Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.
   B. **Subscriber/End-User Use Limitations.** By providing the Scores to Subscriber/End-User pursuant to this Agreement, Provider grants to Subscriber/End-User, a limited license to use information contained in reports generated by the Credit Bureaus/Fair, Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), Subscriber/End-User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the Subscriber/End-User, and (2) identifies Credit Bureaus and Fair, Isaac as express third party beneficiaries of such contract.
   C. **Proprietary Designations.** Subscriber/End-User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations or Provider, Credit Bureaus or Fair, Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

4. **Compliance and Confidentiality**
   A. **Compliance with Law.** In performing this Agreement and in using information provided hereunder, Subscriber/End-User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. Subscriber/End-User certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the Federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the Subscriber/End-User along with the Scores.
   B. **Confidentiality.** Subscriber/End-User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. Subscriber/End-User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, Subscriber/End-User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of Subscriber/End-User and while in transport between the parties. Subscriber/End-User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Credit Bureaus' and Fair, Isaac's express written permission.
   C. **Proprietary Criteria.** Under no circumstances will Subscriber/End-User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Credit Bureaus and/or Fair, Isaac in performing the scoring services hereunder.
   D. **Consumer Disclosure.** Notwithstanding any contrary provision of this Agreement, Subscriber/End-User may disclose the Scores provided to Subscriber/End-User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.

5. **Indemnification and Limitations**
   A. **Indemnification of Provider, Credit Bureaus and Fair, Isaac.** Subscriber/End-User will indemnify, defend, and hold each of Provider, Credit Bureaus and Fair, Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by Subscriber/End-User of any obligations to be performed by Subscriber/End-User under this Agreement, provided that Credit Bureaus/Fair, Isaac have given Subscriber/End-User prompt notice of, and the opportunity and the authority (but not

the duty) to defend or settle any such claim.

B. **Limitation of Liability.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, CREDIT BUREAUS OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO SUBSCRIBER/END-USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USE, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USE WAS ADVISED SUCH DAMAGES ARISE AND OR WHETHER OR NOT END USE WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, CREDIT BUREAUS OR FAIR, ISAAC TO THE SUBSCRIBER/END-USER EXCEED THE FEES PAID BY THE SUBSCRIBER/END-USER PURSUANT TO THIS AGREEMENT DURING THE SIX-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF SUBSCRIBER/END-USER'S CLAIM.

6. **Miscellaneous.**
   A. **Third Parties.** Subscriber/End-User acknowledges that the Scores results from the joint efforts of Credit Bureaus and Fair, Isaac. Subscriber/End-User further acknowledges that each Credit Bureaus and Fair, Isaac have a proprietary interest in said Scores and agrees that either Credit Bureaus or the Fair, Isaac may enforce those rights required.
   B. **Complete Agreement.** This Agreement sets forth the entire understanding of Subscriber/End-User and Provider with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

This Credit Scoring Services Agreement, ("Agreement''), dated: _____ between _____ ("Subscriber/End-User'') and Alliance 2020, Inc. ("Provider'').

IN WITNESS WHEREOF, Subscriber/End-User has signed and delivered this Agreement.

▶ _____ ▶ _____

AUTHORIZED INDIVIDUAL PRINTED NAME TITLE

▶ _____ ▶ _____

AUTHORIZED INDIVIDUAL SIGNATURE DATE

Exhibit A – Businesses Prohibited from Accessing Tenant Screening Credit Reports Under this Agreement

The businesses listed below cannot be provided credit information in keeping with the Fair Credit Reporting Act (FCRA) and the policies of Alliance 2020.

Adult entertainment service of any kind
Businesses that operate out of an apartment or unrestricted location within a residence
Attorney or law offices (except collection attorneys or reports furnished for tenant purposes per the FCRA)
Bail bondsman
Check cashing
Credit counseling
Credit repair clinic or any type of company involved in credit repair activity
Dating service
Financial counseling Genealogical
or heir research firm
Law firm (except collection attorneys or reports furnished for employment purposes per the FCRA)
Massage service
Company that locates missing children
Pawn shop
Private detectives, detective agencies or investigative companies
Individual seeking information for their private use
Company that handles third party repossession Company
or individual involved in spiritual counseling
Subscriptions (magazines, book clubs, record clubs, and other similar businesses.)
Tattoo service
Company seeking Information in connection with time shares
Insurance claims

Addendum: End Use Certification of Compliance California Civil Code – Section 1785.14(a)

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

> Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."
>
> Section 1785.14(a) (2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."
>
> Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, _____ ("End User") hereby certifies to Consumer Reporting Agency as follows (You MUST select by checking either the box IS or the box IS NOT below):

> End User ☐ IS ☐ IS NOT a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

End User also certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

I (we) have read the aforementioned addendum and do hereby agree to all contents.

▶ _____	▶ _____
AUTHORIZED INDIVIDUAL PRINTED NAME	TITLE
▶ _____	▶ _____
AUTHORIZED INDIVIDUAL SIGNATURE	DATE

Addendum to Master Service Agreement
Office of Foreign Asset Control File Indicator Service

Alliance 2020, Inc. agrees to provide, as an add-on service, an indicator whether the consumer's name appears in the United States Department of the Treasury Office of Foreign Asset Control File (OFAC File) as noted below.

1. The provision of the OFAC File Indicator will be in strict accordance with applicable laws and policies, including but not limited to the Fair Credit Reporting Act (FCRA) and the policies of Alliance 2020.

2. The OFAC File Indicator may be provided as exclusion criteria on an input prescreen list, or as an append to a prescreened list.

3. The Subscriber agrees that it is solely responsible for taking any action required by federal law as a result of a match to the OFAC File Indicator

4. This service may be terminated in whole or in part at any time for any reason upon written notice to Subscriber.

5. In the event Subscriber obtains OFAC File Indicator services in conjunction with a consumer report, Subscriber shall be solely responsible for taking any action that may be required by federal law as a result of a match to the OFAC File, and shall not deny or otherwise take any adverse action against any consumer based solely on the OFAC File Indicator service.

Addendum to Master Service Agreement Tenant Screening Access Security Requirements for FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Alliance 2020 systems or data, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Alliance 2020 reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing Alliance 2020's services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Alliance 2020 data:

1. Implement Strong Access Control Measures

1.1 All credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Alliance 2020 will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Alliance 2020's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing Alliance 2020 data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Alliance 2020 data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to Alliance 2020's infrastructure. Each user of the system access software must also have a unique logon password.

1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 Develop strong passwords that are:

i. Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
ii. Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
iii. For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:

I. Any system access software is replaced by another system access software or is no longer used
II. The hardware on which the software resides is upgraded, changed or disposed
III. Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm is utilized (e.g. AES 256 or above). 1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30-minute inactive session timeout.

1.12 Ensure that personnel who are authorized access to credit 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 the membership application.

1.13 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Alliance 2020 data.

1.14 Ensure that Company employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.

1.15 Implement a process to terminate access rights immediately for users who access Alliance 2020 credit 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.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and 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:

I. Use, implement and maintain a current, commercially available anti-virus software e-mail systems, if applicable anti- virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.

II. Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.

III. If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

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 Alliance 2020. data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document 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 Alliance 2020. data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Alliance 2020. data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Alliance 2020. data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Alliance 2020. data via smart tablets or smart phones must protect data

while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Alliance 2020. data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Alliance 2020. data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

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 Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 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. If you believe Alliance 2020. data may have been compromised, immediately notify Alliance 2020. within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).

4.4 The FACTA Disposal Rules requires that Company 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.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Alliance 2020 data, ensure that service provider is compliant with Alliance 2020 Independent Third Party Assessment (EI3PA) program, and registered in Alliance 2020 list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Alliance 2020 and exception is granted in writing. Approved certifications in lieu of EI3PA can be found in the Glossary section.

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 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Alliance 2020 data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access Alliance 2020 systems, access to third party tools/services must require multi-factor authentication.

6.Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Alliance 2020 data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Alliance 2020 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.

7.Mobile and Cloud Technology

7.1 Storing Alliance 2020 data on mobile devices is prohibited. Any exceptions must be obtained from Alliance 2020 in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Alliance 2020 data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Alliance 2020 data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Alliance 2020 data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Alliance 2020:
    - ISO 27001
    - PCI DSS
    - EI3PA
    - SSAE 16 – SOC 2 or SOC3
    - FISMA
    - CAI / CCM assessment

8.General

8.1 Alliance 2020 may from time to time audit the security mechanisms Company maintains to safeguard access to Alliance 2020 information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the Company is accessing Alliance 2020 information and systems via third party software, the Company agrees to make available to Alliance 2020 upon request, audit trail information and management reports generated by the vendor software, regarding Company Individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Alliance 2020 information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Alliance 2020 information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Alliance 2020 systems shall be made available to Alliance 2020 upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Alliance 2020 must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Alliance 2020 to Experian within twenty- four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Alliance 2020 of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatory compliance@experian.com .

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Alliance 2020 services, systems or data, and (d) will abide by the provisions of these requirements when accessing Alliance 2020 data.

8.9 Company understands that its use of Alliance 2020 networking and computing resources may be monitored and audited by Alliance 2020, without further notice.

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Alliance 2020 services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Alliance 2020 data, additional documentation may be required by Alliance 2020.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Alliance 2020 requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Alliance 2020 will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.
"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Alliance 2020 provided services via Internet ("Internet Access").

General Requirements:

1.The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Alliance 2020 on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees 'access to Alliance 2020 provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

2.The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Alliance 2020 product based upon the legitimate business needs of each employee. Alliance 2020 shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.

3.Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Alliance 2020. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Alliance 2020's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Alliance 2020 may add to or change its requirements for granting (Internet)access to the services at any time (including, without limitation, the imposition of fees relating to(Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. Note: Partially completed forms and verbal requests will not be accepted.

4.An officer of the Company agrees to notify Alliance 2020 in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1.Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Alliance 2020 on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Alliance 2020 on information and product access, in accordance with these Alliance 2020 Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Alliance 2020's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Alliance 2020, Inc. immediately.

2.As a Client to Alliance 2020's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.

3.The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Alliance 2020 product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Alliance 2020's Security Administration group on information and product access matters.

4.The Head Designate shall be responsible for notifying their corresponding Alliance 2020 representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.

2.Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).

3.Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

4.Is responsible for ensuring that Company's Authorized Users are authorized to access Alliance 2020 products and services.

5.Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.

6.Must immediately report any suspicious or questionable activity to Alliance 2020 regarding access to Alliance 2020's products and services.

7.Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Alliance 2020, Inc.

8.Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.

9.Shall be available to interact with Alliance 2020 when needed on any system or user related matters.

▶ _____
AUTHORIZED INDIVIDUAL PRINTED NAME

▶ _____
TITLE

▶ _____
AUTHORIZED INDIVIDUAL SIGNATURE

▶ _____
DATE

Glossary Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.

Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven-digit Alliance 2020 account number.
Alliance 2020 Independent Third Party Assessment Program	The Alliance 2020 Independent 3rd Party Assessment is an annual assessment of an Alliance 2020 Reseller's ability to protect the information they purchase from Alliance 2020. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Alliance 2020. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided

Alliance2020
Insight is better than hindsight

Addendum to Master Service Agreement: Tenant Screening End User Data Breach Obligations

As a Subscriber of consumer information you are required to implement and maintain access and security measures to protect this sensitive information from data breaches.

A data breach occurs when sensitive information is stored, delivered, displayed, transmitted or exposed to end user clients and others without permissible purposes in a manner that is inconsistent with or in violation of applicable laws and/or Alliance 2020 policy. Data breaches include, but are not limited to the following events and types of events.

1. Stolen, lost or missing copies of consumer information, including but not limited to paper and electronic copies, including files, backup media, computers, computer hard disks, and other similar items.
2. Online exposure of consumer information online in any fashion, including but not limited to intentional or unintentional E-mail or web browser technology
3. Lost, stolen or exposed passwords
4. Lost or stolen packages and/or correspondence containing consumer information
5. Hacker intrusion into systems that are thought to be secure
6. Establishment of bogus accounts
7. Use of legitimate accounts for fraudulent purposes
8. Unauthorized access to consumer information by a dishonest employee or former employee

If a data breach is suspected to have occurred but has not been confirmed by Alliance 2020, Inc. the Subscriber is responsible to take action in the same manner as if an actual confirmed data breach had occurred. Such action is to continue and progress until such time that Alliance 2020 has notified the Subscriber in writing that the suspected data breach has not occurred.

As a Subscriber you are required to take the following steps with respect to data breaches:

1. Implement formal training consistent with industry standards for all employees and develop and implement in-house procedures.
2. Notify Alliance 2020 of the discovery that a data breach (real or suspected) has occurred within 24 hours of the discovery.
3. Actively and completely cooperate in a timely manner with Alliance 2020 in any investigation into a real or suspected data breach.
4. Notify your end user customer that their personally sensitive information may have been compromised. Alliance 2020 will have control of the nature and timing of consumer correspondence related to the breach when Alliance 2020 information is involved.
5. Cooperate with Alliance 2020 in the implementation of a credit monitoring service for each affected consumer as required.

Alliance2020
Insight is better than hindsight

Addendum to Master Service Agreement: Tenant Screening Consumer Information Disposal Requirements

1. Definitions

   A. As used herein, the term "Consumer Information" shall mean any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

   B. "Dispose," "disposing," or "disposal" means
      (i) The discarding or abandonment of consumer information, or
      (ii) The sale, donation or transfer of any medium, including computer equipment, upon which consumer information is stored.
      (iii) The shredding or burning of fabric or film ribbons used in printers, typewriters and/or copy machines that retain an impression of the image that was printed, transmitted or reproduced.

2. Proper Disposal of Consumer Information

   A. Standard. A person who maintains consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal

   B. Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples
      (i) Implementing and monitoring compliance with policies and procedures that requires the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
      (ii) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
      (iii) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule.
      (iv) For persons who maintain consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (B)(i) and (ii) of this section.

Addendum to Master Service Agreement
Certification that End User will comply with the Fair Credit Reporting Act

Federal Fair Credit Reporting Act (as amended by the Consumer Credit Reporting Reform Act of 1996)

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of consumer information. The FDRA may be acquired online by accessing the Federal Trade Commission website at ftc.gov. We suggest that you and your employees become familiar with the following sections in particular:

§ 604. Permissible Purposes of Reports
§ 607. Compliance Procedures
§ 615. Requirement on users of consumer reports
§ 616. Civil liability for willful noncompliance
§ 617. Civil liability for negligent noncompliance
§ 619. Obtaining information under false pretenses
§ 621. Administrative Enforcement
§ 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies

Each of these sections is of direct consequence to users who obtain reports on consumers.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, and other lawful and permissible uses It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.

Alliance 2020 supports legislation that will assure fair and equitable treatment for all consumers and users of credit information.
Customer certifies that it will comply with applicable provisions of the Federal Fair Credit Reporting Act.

I (we) have read the aforementioned addendum and do hereby agree to all contents.

▶ _____
AUTHORIZED INDIVIDUAL PRINTED NAME

▶ _____
TITLE

▶ _____
AUTHORIZED INDIVIDUAL SIGNATURE

▶ _____
DATE

Master Death File Index Addendum

Access to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. §1110.102(a)(1).

The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). As many Alliance 2020, Inc. services contain information from the DMF, Alliance 2020, Inc. would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the Alliance 2020, Inc. services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with your applicable Fair Credit Reporting Act (15 U.S.C. §1681 *et seq.*) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*) use. Your continued use of Alliance 2020, Inc. services affirms your commitment to comply with these terms and all applicable laws.

Subscriber/End-User shall indemnify and hold harmless Alliance 2020, Inc., TransUnion, Equifax, Experian and the US Government / NTIS from all claims, demands, damages, expenses and losses whether sounding in tort, contract or otherwise, arising from or in connection with Subscriber/End-Users' use of the Master Death File.

Subscriber/End-User Name: _____ acknowledges you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Alliance 2020, Inc. services.

▶ _____
AUTHORIZED INDIVIDUAL PRINTED NAME

▶ _____
TITLE

▶ _____
AUTHORIZED INDIVIDUAL SIGNATURE

▶ _____
DATE

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

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. 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 website. Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.

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

I. Obligations of All Users of Consumer Reports

A. Users Must Have a Permissible Purpose

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

- As ordered by a court or 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. Section 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 or 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 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 the 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 subject 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 below.
- Upon written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. Special Procedures for Employee Investigations

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

VI. Obligations of Users of Medical Information

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

VII. Obligations of Users of "Prescreened" Lists

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Section 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. This statement must include the address and the toll-free telephone number of the appropriate notification system.

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

VIII. Obligations of Resellers

A. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:

  1) the identity of all end-users;

  2) certifications from all users of each purposes for which reports will be used; and

  3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. Liability for Violations of The FCRA

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

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

Citations for the 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

Alliance 2020
Insight is better than hindsight

Addendum to Master Service Agreement
On-Site Inspection Acknowledgement and Agreement

In order to process your new subscriber account with Alliance 2020 an onsite inspection is required. This new policy has been set forth by the Credit Bureaus as a result of recent media attention regarding a wide range of data breaches. This has caused heightened security concerns by consumers, legislators, regulators and businesses. These incidents emphatically underscore the need for all organizations to review current business practices to specifically improve information security and protection of sensitive consumer data.

Alliance 2020 has a well-earned reputation as a responsible steward of the highly proprietary and sensitive personal information under its care. We take this role very seriously and invest heavily to ensure that our information is maintained in a safe and secure environment, used in a manner consistent with the requirements of state and federal laws and our own stringent business practices. We provide information only to end-users who have legitimate and permissible purpose for access, use and security of the data.

Alliance 2020 is now required by the Credit Bureaus to employ the services of an approved, vendor to conduct the required physical inspection of your company if you are a company or individual accessing consumer credit information for tenant screening purposes

Alliance 2020 charges a one-time onsite inspection fee for all new subscriber locations, including branch offices to help defray the expense of setting up an account. Upon receipt of your application (typically the same business day), an Alliance Customer Service representative will contact you to collect payment for this service in advance. If required, this fee is non-refundable.

The items that the onsite inspection firm will inspect are described briefly on the next page. There are separate requirements for businesses located in commercial settings and for those operating out of private residences. Alliance does not currently provide service to subscribers doing business out of apartments or condominiums.

You will be contacted by a representative of independent inspection firm to schedule an appointment for your onsite inspection and to collect the fee for the inspection. The fee can be paid by credit card to expedite the process. The inspection only takes 10 or 15 minutes, and will typically be completed within three days of the receipt of your inspection fee payment.

Inspection Checklist

An onsite physical inspection will be undertaken at your location for the purpose of performing due diligence by Alliance 2020. The inspection will include at least two photographs of your location, including the interior and exterior. All information acquired in the inspection will be kept confidential.

You will be contacted in advance to schedule this inspection by an independent, third-party inspection firm. You are encouraged to verify the identity of the inspector, and to contact Alliance 2020 if you have any questions about the inspection or the inspector.

The lists below are summaries of the items that may be audited and/or scrutinized. This list is not intended to be comprehensive, but is provided as a guide. The inspection may include the verification of items on your application and examination of your facilities with respect to security and compliance with other Bureau policies, as detailed in your application packet.

A separate list is provided for commercial locations and residential locations. In every case, the inspector will make the determination if the location is a commercial location or a residential location.

Commercial Location Inspection Items	**Residential Location Inspection Items**
Determine if the office space is shared with other businesses and/or is an executive suite with a shared receptionist.	Determine if the location is in an apartment or high-rise condominium.
If the location is shared, determine if the individual offices are separately locked.	Determine if the work area is physically separated from the living quarters.
Determine if prohibited businesses are operating at or adjacent to the business location.	Determine if prohibited businesses are operating at or adjacent to the business location.
Determine if there is evidence of displayed business license(s) as required by law.	Determine if there is evidence of displayed business license(s) as required by law.
Examine confidential document storage (locked) and destruction facilities/general office observations	Examine confidential document storage (locked) and destruction facilities/general office observations.
Record the method of receiving reports and location/security of equipment.	Record the method of receiving reports and location/security of equipment.
Confirm that the address on application matches the property address.	Confirm that the address on application matches the property address.