SureRent 2020 Private Landlord
Tenant Screening Application Package

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.

IMPORTANT LIMITATION

Information provided under this agreement must be used only for the purpose of evaluating prospective tenants for rental or leasing of real property. Such information is provided at the request of the consumer. Alliance 2020 reserves the right to audit your files to verify your use of the credit reports provided under this agreement.

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

Required Forms

The forms listed below are part of this agreement, and must be read, understood. When you sign the attached agreement, you agree to understand and abide by these provisions.

- Facts You Need to Know!
- Private Landlord Application for Service for Tenant Screening Services
- Access and Security Requirements
- Data Breach Obligations
- Requirements for the Disposal of Consumer Information
- Fair Credit Reporting Act (FCRA) Requirements for Subscribers

Other Information/Training

Your packet includes a number of pages with important information. You should read and understand this information as your acceptance of these items is part of the agreement you are signing. You are responsible to follow all laws with respect to the use of consumer information and the rental/leasing of residential property.

A customer service representative will contact you within one business day of receipt of your application for service to perform our required due diligence and arrange for training on our online system.

FACTS YOU NEED TO KNOW!

Caution! Tenant Screening is a Regulated Activity!

Screening to determine suitability for residency is strictly regulated by both Federal and state laws. This is true even if all you want to do is rent a room to a college student. Non-compliance with these laws can result in civil and criminal penalties. By using Alliance 2020, you are assured that your report is fully compliant with existing laws.

Because of the legal requirements, the initial establishment of your screening account requires Alliance 2020 to perform a certain level of due diligence. Due diligence is the process of verifying your identification, and determining that you have a permissible purpose for acquiring the information Alliance 2020 can provide. We go through a multiple step process to perform due diligence, and ask for copies of documents that assure us of your identity and your legitimate need for background information. Our process includes contacting you in person. As a result, it takes an average of 24 business hours to set up a screening account. Once your account is set up, you can log in and acquire a report at any time, with typical results returned in just a few minutes. County-level criminal results, in some instances, may take additional time.

Screening Packages We Offer

Alliance 2020 offers a range of screening packages to meet the needs of the Private Landlord. Each of these packages are available at any time -- you choose the package you need.

The Account Setup Process

The account setup is a simple process that you complete ONCE. You read and agree to our terms and conditions, fill out our online application for a tenant screening account and submit the information with your signature. Alliance 2020 will perform its due diligence, contact you with a user name and password and train you to use our screening system. From that time forward you will be able to access our state-of-the-art screening system and run professional background checks on applicants or prospective roommates.

One-Time Set Up Fee

Alliance 2020 charges a one-time fee of $49.95 to defray our costs for due diligence. This fee is non-refundable. After you are set up, you only pay for the reports you order.

Private Landlord Application for Service for Tenant Screening Services

Personal Information

Your Full Name_____ SSN_____

Address _____City _____ State _____ Zip_____

Date of Birth _____ Email Address _____Cell Phone_____

How did you hear about Alliance 2020?_____

Your Government Issued Photo ID

We require you to provide us with a government-issued photo ID to assist us in our due diligence process. The ID you provide allows us to establish your identity. The information you provide here will not be shared with any third party, except as required by law or in response to an order from a court of law.

Type of ID:

☐ Driver's License ☐ State ID Card ☐ Passport ☐ Military ID ☐ Other (Explain Below)

Other Explanation _____

ID No. _____ State of Issue _____

Full Name as it Appears on the ID _____ Date Expires _____

Address on the ID _____City _____ State _____ Zip_____

YOU MUST ATTACH A READABLE PHOTOCOPY OR SCAN OF THE ID

I acknowledge that I have read and understand the account agreement and other documents contained as part of Alliance 2020s' agreement package and I agree to be bound by their terms and conditions. I certify that all information I have provided is true and correct, and that I am the individual named in this agreement. I understand that I may not resell the information provided by Alliance 2020 or share it with any third party.

I have read and understood the attached Agreement, and I intend to rely upon it and understand that Alliance 2020 will rely upon it, and I intend to be bound thereby.
I acknowledge and agree that it is my obligation to immediately advise Alliance 2020 of any change in my physical or electronic address (i.e., E-mail address).

Signature _____ Date _____

Printed Name _____ Daytime Telephone _____

Your Rental Properties

We require you to provide us with a list of the rental properties for which you will be screening applicants, even if it is only one unit. We will verify your ownership of these properties, and you will be required to list the property address on the application form you give the applicant to fill out. Alliance 2020 will provide you with blank application forms after you sign up.

List your rental property addresses below.

Address _____

City _____ State _____ Zip_____

Address _____

City _____ State _____ Zip_____

Address _____

City _____ State _____ Zip_____

Address _____

City _____ State _____ Zip_____

Address _____

City _____ State _____ Zip_____

Signature_____ Date _____

Access and Security Requirements

Each person or business that uses or provides credit information and/or consumer information must work together to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of consumer credit reports. As a client of Alliance 2020, you agree to follow these and other reasonable measures in accessing and storing credit information.

1. Implement formal training consistent with industry standards for all employees that includes a signed certification from the employee that the training has taken place.

2. Develop and implement a procedure for notifying Alliance 2020 of a the discovery of a data breach (real or suspected) within 24 hours, including the following actions

   (A) Actively and completely cooperate in a timely manner with Alliance 2020 in any investigation into a real or suspected data breach
   (B) 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.
   (C) Cooperate with Alliance 2020 in the implementation of a credit monitoring service for each affected consumer

3. You must protect your account number and password so that only key personnel employed by your company know this sensitive information. Unauthorized persons should never have knowledge or be able to access your password. Do not post this information in any manner within your facility. If a person who knows the password leaves your company or no longer needs to know it due to a change in duties, the password should be deleted and the account locked immediately by the Subscriber's administrator. If the Subscriber cannot lock the account or delete the password Alliance 2020 must be notified at once.

4. System access software, whether developed by your company or purchased from a third party vendor, must have your account number and password "hidden" or embedded and be known only by supervisory personnel. You must assign each user of your system access software a unique logon password. If such system access software is replaced by different access software and therefore no longer in use or, alternatively, the hardware upon which such system access software resides is no longer being used or is being disposed of, your password should be changed immediately.

5. Do not discuss your account number and password by telephone with any unknown caller, even if the caller claims to be an employee of your credit provider.

6. Restrict the ability to obtain credit information to a few key personnel.

7. Place all terminal devices used to obtain credit information in a secure location within your facility. You should secure these devices so that unauthorized persons cannot easily access them.

8. After normal business hours be sure to turn off and lock all devices or systems used to obtain credit information.

9. Secure hard copies and electronic files of consumer reports within your facility so that unauthorized persons cannot easily access them.

10. Shred or destroy all hard copy consumer reports when no longer needed.

11. Shred, burn or otherwise destroy any fabric or film ribbons used in printers, typewriters and/or copy machines that retain an impression of the image that was printed, transmitted, displayed or reproduced.

12. Erase and overwrite or scramble electronic files containing consumer information when no longer needed and when applicable regulation(s) permit destruction.

13. It is recommended that hard drives used to store or process consumer information be low-level formatted or physically pulverized when they are removed from service.

14. Keep informed and follow Alliance 2020 requirements for restricting access to system access software from limited Internet Protocol (IP) addresses.

15. Install, implement and maintain appropriate virus, malware, spyware and adware tools on your servers and workstations to ensure security.

16. Make all employees aware that your company can access credit information only for the permissible purposes listed in the Permissible Purpose Information section of your subscription application.

17. You or your employees may not access their own reports for any reasons. Nor should you or your employees access the report of a family member or friend unless it is in connection with a credit transaction or for some other permissible purpose.

18. Record Retention: The Federal Equal Opportunities 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 and its providers 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 and its providers 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 $2,500 per violation."

Client agrees to implement and adhere to the above access security controls.

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, 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.

Client agrees to implement and adhere to the above steps with respect to data breaches.

Requirements for the Disposal of Consumer Information

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. An 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.

Client agrees to implement and adhere to the above steps with respect to data disposal.

Fair Credit Reporting Act (FCRA) Requirements for Subscribers

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. We have included a copy of the FCRA with your membership kit. 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.

Client acknowledges agreement to abide by the FCRA and all other applicable laws.