# FAST and EASY ACCESS
# to Tenant Screening

## FOUR SIMPLE steps to get you started:

**STEP 1** Submit the required documents for the credit bureau(s) of your choice

**STEP 2** Complete the End User Application

**STEP 3** Sign the Credit Report Service Agreement & FCRA Requirements

**STEP 4** Sign the Access Security Requirements & Credit Scoring Agreement

AOA is required by state and federal law to investigate and validate the legitimate business of the member who has a need for a consumer credit profile. Attached, please find the forms necessary to meet the compliance mandates. These documents serve three basic purposes:

- To show that you are compliant under the Fair Credit Reporting ACT (FCRA).
- To confirm that you are an approved business (individual Owner/Landlord, LLC or Property Management Company) and have a permissible purpose under federal FCRA law to request credit reports.
- Your acknowledgment of federal credit reporting laws and policies in place to protect tenants from fraud and identity theft.

THE FCRA IMPOSES CRIMINAL PENALTIES – INCLUDING A FINE, UP TO TWO YEARS IN PRISON, OR BOTH – AGAINST ANYONE WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES, AND OTHER PENALTIES FOR ANYONE WHO OBTAINS SUCH CONSUMER INFORMATION WITHOUT A PERMISSIBLE PURPOSE. OTHER APPLICABLE LAWS MAY IMPOSE SIMILAR PENALTIES.

**Email to:**
aoa.crsa@aoausa.com
**Fax to:**
Compliance Relations Team at (818) 936-6703
**Mail to:**
AOA Compliance Relations 6445 Sepulveda Blvd. #300, Van Nuys, CA 91411
**Contact:**
For all compliance questions please call: (800) 827-4262 Monday - Friday, 8:30 A.M. – 5:00 P.M.

Thank you for working with us to meet the requirements of the credit bureaus.

# **STEP 1** - Submit the required documents

If you are an individual property owner, property management company, rental corporation or real estate broker/firm, please submit the following:

**1.** Clear copy of your driver's license.
**2.** A voided check, bank deposit slip, or bank statement.
**3.** The phone bill with the contact name, number and address you have provided us.
**4.** If you are operating under a business name, also send ONE of the following: business license, LLC documents, proof of fictitious name filing, federal tax ID, or trust documents.
**5. FOR TRANSUNION:** If you have been in business for LESS than ONE year, please also submit a utility bill for the physical street address location (the office/where the files are located).
**6. FOR EXPERIAN OR ABC GRADE REPORT, PLEASE ALSO SUBMIT:** One completed and signed rental application or lease agreement for each rental property. (If you own more than 3 rental properties or if you are a management company, simply submit 3 rental applications or lease agreements).
**7. FOR EXPERIAN OR ABC GRADE REPORT, PLEASE ALSO SUBMIT:** One tax bill or property insurance for each rental property for proof of ownership. Management companies do not need to submit proof of ownership.

**Please select the credit bureau(s) of your choice**
AOA recommends that you obtain authorization for full detailed reports

## ☐ Transunion Full Credit Report

If you are operating from a **commercial** or **residential** location, a **one-time** on-site visit is required.

## ☐ Experian Full Credit Report

If you are operating from a **residential location,** an on-site visit is required annually. If you are operating from a **commercial location,** a one-time on-site visit is required.

## ☐ ABC Grade Report

You do not need an on-site visit when using the ABC report only.

For full access to credit reports, a site inspection is REQUIRED by the credit bureaus.
This tax-deductible $59.00 fee for the onsite inspection applies to both credit bureaus.

**Thank you for working with us to meet the requirements of the credit bureaus!**




San Fernando Valley (818)988-9200 Los Angeles (323)937-8811 Long Beach (562)597-2422 Garden Grove (714)539-6000 San Diego (619)280-7007 Northern California (510)769-7521

# **STEP 2** - Complete End User Application

## General Company/Individual Information

Type of Ownership (indicate one): ☐ Individual Owner/Landlord ☐ Management Company ☐ Apartment Rental Corporation ☐ LLC

Company/Individual Name: _____

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

Where Files/Office are Located (no P.O. box numbers, please)

Physical Street Address : _____

City: _____ State: _____ ZIP: _____ How Long? _____ yrs _____ mos.

Is this a residential address? ☐ Yes ☐ No If Yes, does the residence have a gated community entrance? ☐ Yes ☐ No

Previous Address: _____

City: _____ State: _____ ZIP: _____ How long? _____ yrs _____ mos.

## Principal of the Company or Individual Owner

Principal name: _____ Title or Position: _____

Current Residential Street Address: _____

City: _____ State: _____ ZIP: _____

Social Security Number: _____ Tax ID Number: _____

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

Years in Business: _____Yrs. _____ Mos. Number of rental properties you own/manage:_____ Units:_____

## Business Information or Individual Owner

Tel: _____ Fax:_____Email Address _____

Type of Business (i.e. rental): _____ Anticipated monthly credit reports: _____

Will access be primarily: ☐ Local ☐ Regional ☐ National How will you access the Credit Reports? ☐ Online Access ☐ Call Center ☐ Fax

Website Address: _____

## Permissible Purpose/Appropriate Use

Please describe the specific purpose for which credit information will be used. (What will you do with the information obtained?)

This section MUST be completed. _____

_____

_____

The following applies to consumer credit products (i.e. Consumer Credit Reports, Business Owners Profile, and Small Business Intelliscore): I have read and understand the "Credit Report Service Agreement/FCRA Requirements" notice and "Access Security Requirements/Credit Scoring Services Agreement" and will take all reasonable measures to enforce them within my facility. I certify that I will use the Credit Reporting Agency's product information for no other purpose other than what is stated in the Permissible Purpose on the letter of Intent and for the type of business listed on this application. I will not resell the report to any third party. I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated. I certify that the above information is accurate and hereby authorize the release information to AOA for the establishment of opening an account. I also acknowledge that a site inspection of my place of business will be required to complete compliance procedures. I understand that the information provided in this application may be used to obtain a consumer credit report, and my creditworthiness may be considered when making a decision to grant end user access.

_____ _____ _____

Signature/Title Membership Number Date





San Fernando Valley (818)988-9200 Los Angeles (323)937-8811 Long Beach (562)597-2422 Garden Grove (714)539-6000 San Diego (619)280-7007 Northern California (510)769-7521

# STEP 3
# Credit Report Service Agreement & FCRA Requirements

AOA Member Name/Company _____, herein referred to as "Member" declares, certifies and agrees as follows:

1. Member is an "end user" of credit data and uses such data for the permissible purposes stated in this agreement. Member will certify the purpose for which each credit report is requested at the time of the inquiry. Each request for employment purposes will be so designated at the time of the request and a separate service agreement must be completed for certifications of compliance with the Fair Credit Reporting Act (FCRA). Member will neither resell nor distribute credit data obtained from AOA, TransUnion (TU), Experian (XPN), and/or any of its Affiliates to any third party. Member is aware that to do so would violate AOA's, TU's, and XPN's company policy and certain provisions of state and federal law. Member understands that information provided will be maintained in a secure file, be held strictly confidential and not sold or supplied to any third parties or affiliates. Member shall receive and maintain all credit data in strict confidence and will not reveal its contents to the consumer unless compelled by law. Member further agrees to only use Consumer Report for a one-time use.

2. **Member's rental and/or employment application contains the consumer's signature clearly and conspicuously authorizing member to obtain a credit report** and states the address of the rental property. Member is also aware that pursuant to the Fair Credit Reporting Act (FCRA) a fine under Title 18 of $5,000 and/or imprisonment not more than two years or both may result from requesting a consumer credit report under false pretenses and/or a **$3,500 fine** pursuant to state law for each violation (ww.ftc.gov). **Member agrees to comply with all applicable federal, state and local laws, including the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681 et seq.**

3. **Member and member's employees will not access consumer credit data on themselves, friends and/or family members. Member shall only run reports on his/her/its employees for employment purposes only through an authorized and designated representative and not by the subject employee.**

4. Member will maintain adequate security with reference to access and use of membership numbers, subscriber codes, security passwords, consumer data and remote computer access capabilities to prevent unauthorized use and ensure confidentiality.

5. Member agrees to defend and hold AOA, TU, XPN, and/or any of its Affiliates their employees and agents, harmless on account of any expense or damages arising out of Member's or Member's employee's or agent's breach of any of the terms herein or violation of any law applicable hereto.

6. Member agrees that an on site inspection must be made of member's place of operation along with 3 photos to help verify compliance with this agreement.

7. Member recognizes that information is secured by and through fallible human sources and that for the fee charged AOA, TU, XPN, and/or any of its Affiliates cannot be an insurer of the accuracy of the information. Member understands that the accuracy of the information furnished by said providers is not guaranteed and Member releases said providers and their employees, agents and independent contractors from liability for any loss or expense suffered as a result of any inaccuracies, errors or omissions in said information.

8. Member agrees that upon request from AOA, member will supply to AOA qualifying documents to verify ownership and/or management of rental units, etc., as required by TU, XPN, and/or any of its Affiliates to be renewed every three years or when member changes location. Member will preserve all applications and other consumer documents for five (5) years from the date of the inquiry whether the application is accepted or rejected. Member will make all said documents available to AOA.

9. Member agrees to pay all charges with the authorized credit card on file. Pursuant to Section 1785.26 of the California Civil Code, as required by law, you are hereby notified that a negative credit report reflecting on your credit record may be submitted in the future to a credit reporting agency if you fail to fulfill the terms or default in anyway of your credit obligations to AOA. Member expressly authorizes AOA (including a collection agency) to obtain a consumer credit report, which AOA may use for the processing of membership application and/or for debt collections. With just cause, such as payment delinquency or violation of the terms of this contract or a legal requirement, AOA may, upon its election, discontinue all membership services to Member and cancel this Agreement immediately by oral or written notice. Member agrees to all terms of this agreement.

Federal Fair Credit Reporting Act (FCRA-Public Law 91-508)

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. 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 of 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

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 investment, partnership, etc. 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. 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 require that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate. AOA strongly endorses 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. We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information. We encourage you to view these laws on the Federal Trade Commission's web site at: www.ftc.gov.

_____ _____ _____

Signature/Title Membership Number Date

# STEP 4

# ACCESS SECURITY REQUIREMENTS & CREDIT SCORING SERVICES AGREEMENT

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to TU/XPN systems or data through AOA, 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. AOA 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 AOA'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 TU/XPN 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 AOA will ever contact you and request your credentials.
1.2 If using third party or proprietary system to access AOA'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 AOA data/systems.
1.3 If the third party or third party software or proprietary system or software, used to access AOA 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 AOA'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:
- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- 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:
- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- 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 are 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 TU/XPN 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 TU/XPN 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:
- Use, implement and maintain a current, commercially available anti-virus software on all 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.
- 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.
- 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 TU/XPN 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 TU/XPN 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 TU/XPN 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 TU/XPN data, ensure that such devices are protected via device pass-code.
3.7 Applications utilized to access TU/XPN 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 TU/XPN 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 TU/XPN 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 TU/XPN data may have been compromised, immediately notify AOA 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 TU/XPN data, ensure that service provider is compliant with TU/XPN Independent Third Party Assessment (EI3PA) program, and registered in TU/XPN 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 TU/XPN 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 TU/XPN 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 AOA 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 TU/XPN 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 AOA 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 TU/XPN data on mobile devices is prohibited. Any exceptions must be obtained from TU/XPN 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 TU/XPN 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 TU/XPN 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 TU/XPN 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 TU/XPN:
♦ ISO 27001 ♦ PCI DSS ♦ EI3PA ♦ SSAE 16 – SOC 2 or SOC3 ♦ FISMA ♦ CAI / CCM assessment

## 8. General

8.1 AOA may from time to time audit the security mechanisms Company maintains to safeguard access to TU/XPN 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 TU/XPN information and systems via third party software, the Company agrees to make available to AOA 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 AOA 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 AOA 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 AOA systems shall be made available to AOA upon request, for example during breach investigation or while performing audits
8.6 Data requests from Company to AOA 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 TU/XPN to AOA within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to AOA 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 at 818-988-9200, Email notification is preferred and will be sent to aoa.crsa@aoausa.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 AOA services, systems or data, and (d) will abide by the provisions of these requirements when accessing TU/XPN data.
8.9 Company understands that its use of AOA networking and computing resources may be monitored and audited by AOA, 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 AOA 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 TU/XPN data, additional documentation may be required by AOA.
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, TU/XPN 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, TU/XPN 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 AOA 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 AOA on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to AOA 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 AOA product based upon the legitimate business needs of each employee. AOA 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 AOA. 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). AOA's approval of requests for (Internet) access may be granted or withheld in

its sole discretion. AOA 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 AOA 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 AOA 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 AOA on information and product access, in accordance with these TU/XPN 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 AOA's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to AOA immediately.
2. As a Client to AOA'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 AOA 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 AOA's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding AOA 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 AOA 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 AOA regarding access to AOA's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to AOA.
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 AOA when needed on any system or user related matters.

**Important Notice – Death Master File**

**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 TU/XPN services contain information from the DMF, TU/XPN would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the TU/XPN 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 TU/XPN services affirms your commitment to comply with these terms and all applicable laws.
You acknowledge 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 TU/XPN services.
End User shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by AOA; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by AOA , (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

## Credit Scoring Services Agreement

The End User hereby agrees to the following:
(i) The End User warranties that it has a "permissible purpose" under the Fair Credit Reporting Act, as it may be amended from time to time, to obtain the information derived from the TU/XPN/Fair, Isaac Model.
(ii) The End User agrees to limit its use of the Scores and reason codes solely to use in its own business with no right to transfer or otherwise sell, license, sublicense or distribute said Scores or reason codes to third parties;
(iii) A requirement that each End User maintain internal procedures to minimize the risk of unauthorized disclosure and agree that such Scores and reason codes will be held in strict confidence and disclosed only to those of its employees with a "need to know" and to no other person;
(iv) Notwithstanding any contrary provision of this End User Agreement, End User may disclose the Scores provided to End User under this End User Agreement to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only.
(v) A requirement that each End User comply with all applicable laws and regulations in using the Scores and reason codes purchased from Reseller;
(vi) A prohibition on the use by End User, its employees, agents or subcontractors, of the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of TU/XPN Information Solutions, Inc. or Fair, Isaac and Company, or the affiliates of either of them, or of any other party involved in the provision of the TU/XPN/Fair, Isaac Model without such entity's prior written consent;
(vii) A prohibition on any attempts by End User, in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by TU/XPN/Fair, Isaac in performing the TU/XPN/Fair, Isaac Model;
(viii) Warranty. TU warrants that the TU Model and XPN/Fair, Isaac warrants that the XPN/Fair, Isaac Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the TU/XPN/Fair, Isaac Model was developed, the TU/XPN/Fair, Isaac Model score may be relied upon by Reseller and/or End Users to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to End Users. TU/XPN/Fair, Isaac further warrants that so long as it provides the TU/XPN/Fair, Isaac Model, it will comply with the regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 et seq. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES TU/XPN/FAIR, ISAAC HAVE GIVEN RESELLER AND/OR END USERS WITH RESPECT TO THE TU/XPN/FAIR, ISAAC MODEL AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, TU/XPN/FAIR ISAAC MIGHT HAVE GIVEN RESELLER AND/OR END USERS WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Reseller and each respective End User's Rights under the foregoing Warranty are expressly conditioned upon each respective End User's periodic revalidation of the TU/XPN/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.).
(ix) A provision limiting the aggregate liability of Reseller, TU/XPN/Fair, Isaac to each End User to the lesser of the Fees paid by Reseller to TU/XPN/Fair, Isaac for the TU/XPN/Fair, Isaac Model resold to the pertinent End User during the six (6) month period immediately preceding the End User's claim, or the fees paid by the pertinent End User to Reseller under the Resale Contract during said six (6) month period, and excluding any liability of Reseller, TU/XPN/Fair, Isaac for incidental, indirect, special or consequential damages of any kind.

**Some of the technical requirements stated in this form may not apply to all end users but must be included into our Access Security Requirements Form/Credit Scoring Services Agreement as directed by the Credit Reporting Agency.**

**It is important that you keep all rental/employment applications for a minimum of five years.** This will help to facilitate the investigative process should a consumer claim that you inappropriately accessed their credit report. By signing below, you acknowledge receipt of the policies listed on this document. You further acknowledge that you read, understand, and agree to implement and adhere to the above controls.

| Signature/Title | Membership Number | Date |
|---|---|---|

# Rental Property List

## Every rental property must include property name, address, contact and phone number

| Property Name | Address | Contact | Phone |
|---|---|---|---|
| Ex: The Palms Apts. | 1234 First St. Los Angeles CA, 90055 | John Smith - Manager | (555) 555 - 5555 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Signature/Title _____ Membership Number _____ Date _____